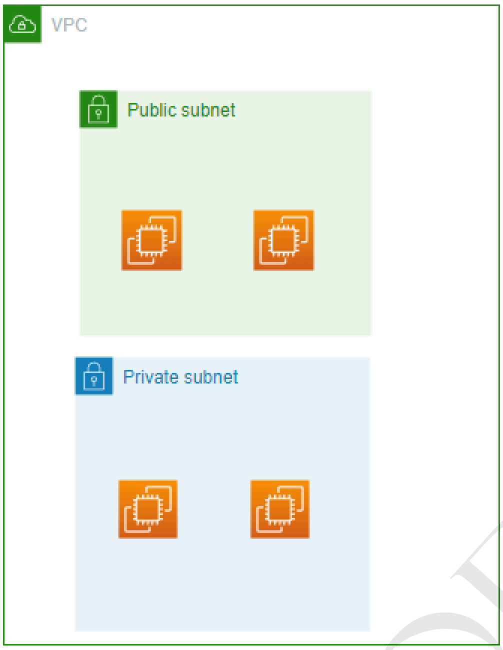
Domain - Technology - Core Services - EC2

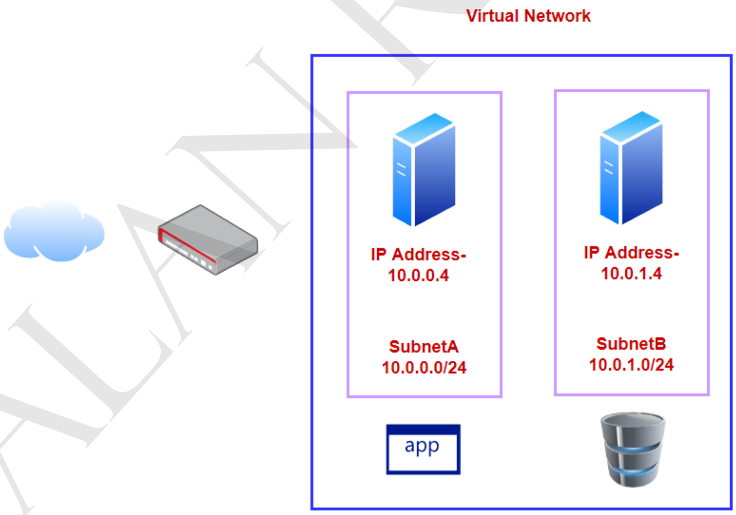
About the Amazon VPC service

Amazon VPC



This is an isolated network on the cloud

You can launch EC2 Instances within a VPC



Sample network deployment

Normally Server Machines

Red Hat Linux

Ubuntu Linux

Windows Server 2019/2022

The IP address helps to uniquely identity each machine on the network

Default VPC

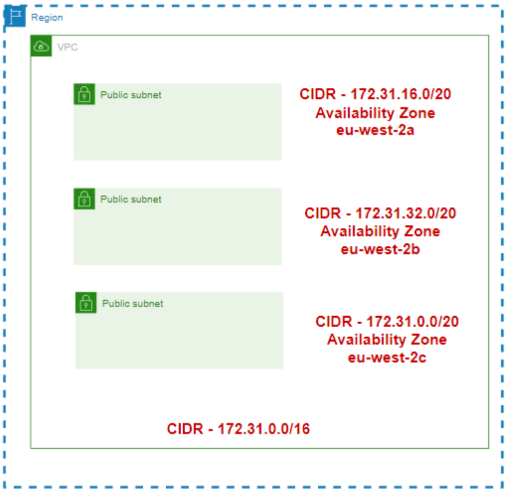
A default VPC is created in each region

The default VPC has a public subnet in each Availability Zone

It has an Internet Gateway

You can easily launch an EC2 Instance in the default VPC

London



CIDR - 172.31.16.0/20
Availability Zone
eu-west-2a

CIDR - 172.31.32.0/20
Availability Zone
eu-west-2b

CIDR - 172.31.0.0/20
Availability Zone
eu-west-2c

CIDR - 172.31.0.0/16

CIDR - Classless Inter-Domain Routing

Its just a way of representing an IP address and a network mask

Lab - Launching an EC2 Instance

Default VPC

London

Public IP

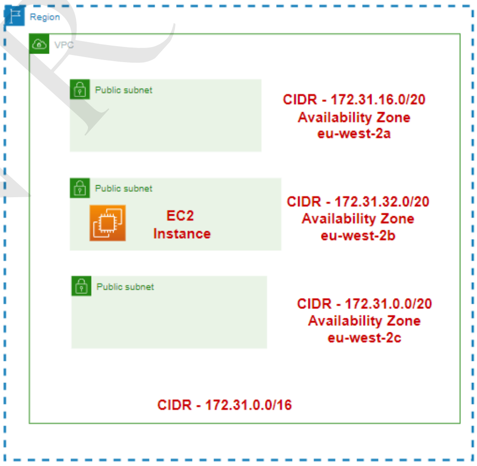
This allows your instance to be reachable from the Internet.

Security group

This controls the traffic that is inbound and outbound from a resource. Rules are present to control the traffic.

Elastic network interface

This is used to represent a virtual network card.



CIDR - 172.31.16.0/20
Availability Zone
eu-west-2a

CIDR - 172.31.32.0/20
Availability Zone
eu-west-2b

CIDR - 172.31.0.0/20
Availability Zone
eu-west-2c

CIDR - 172.31.0.0/16

AMI
Amazon Machine Image

The image has the information required to launch an instance.

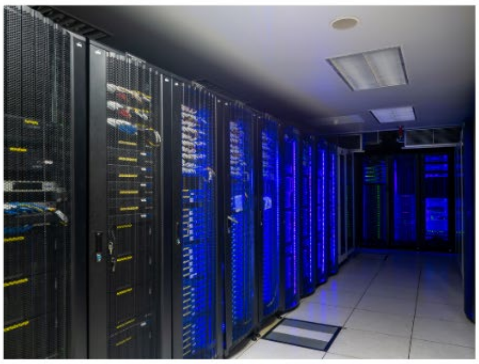
Instance type

This is a combination of CPU, Memory, Storage, Networking and other capabilities

Key Pair

This is a combination of a public and private key. The public key is stored on your Linux-based instance. You use the private key to securely SSH into the instance.

Regions and Availability zones

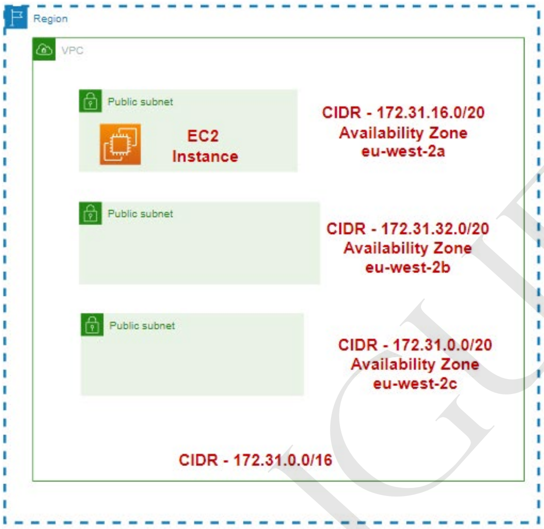


In the virtual infrastructure needs to be located somewhere

The virtual infrastructure is just made available to you via the Internet

Default VPC

London



CIDR - 172.31.16.0/20
Availability Zone
eu-west-2a

CIDR - 172.31.32.0/20
Availability Zone
eu-west-2b

CIDR - 172.31.0.0/20
Availability Zone
eu-west-2c

CIDR - 172.31.0.0/16

There are some services that are available at a global level

Which region should you choose for hosting your resources?

1. Cost of services differ from region to region

2. The location of your users

3. Data sovereignty

4. Does the service exist in that region.

AWS Data Center

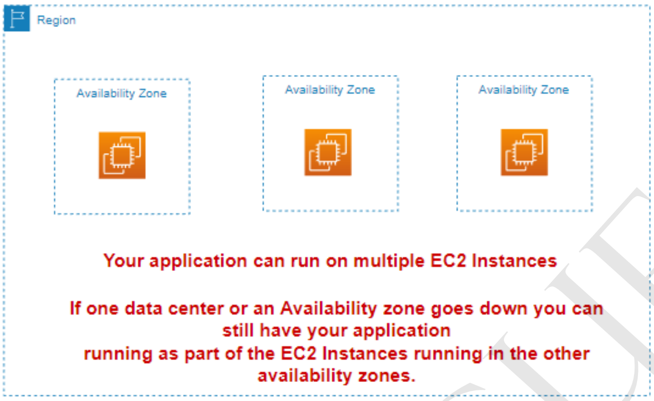
What happens if the data center goes down

EC2 Instance

Availability zones

Availabilty zones is one or more discrete data centers

They have their own redudant power, networking and connectivity in an AWS region.



Your application can run on multiple EC2 Instances

If one data center or an Availability zone goes down you can still have your application running as part of the EC2 Instances running in the other availability zones.

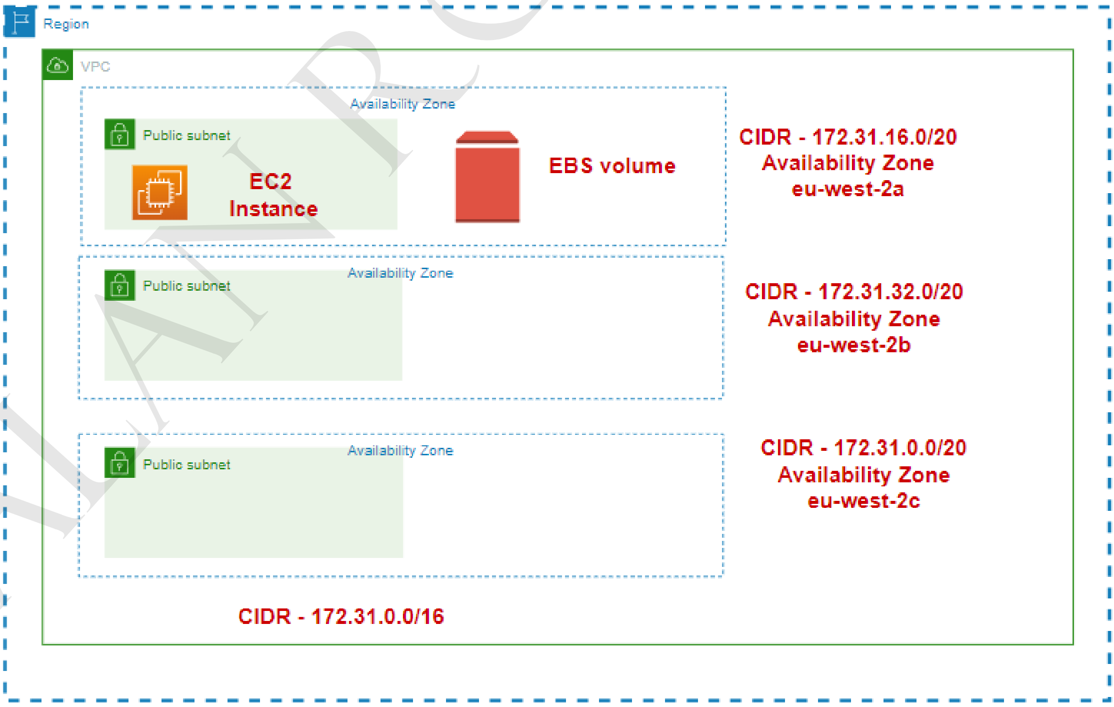
Concept - High Availability

Domain - Technology - Core Services – Storage

About EBS Volumes

Default VPC

London



This is durable, block-level storage devices that can be attached to instances.

The EBS volumes can be mounted as devices on the instances.

You can then create a file system on the volumes.

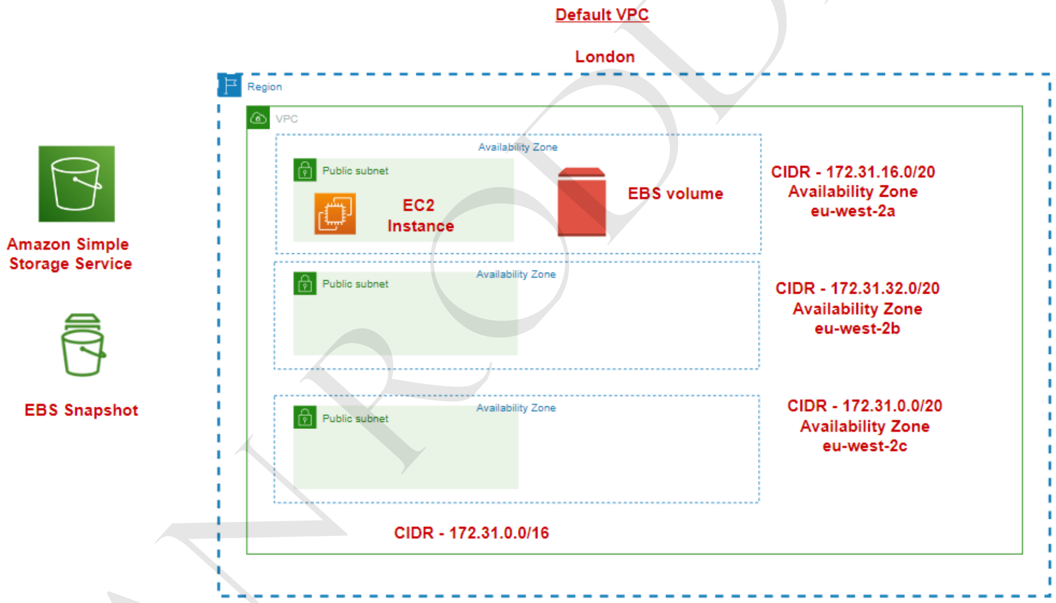
The volumes can persist even after the instance is terminated.

You can attach multiple volumes to an EC2 Instance.

The volume and instance must be in the same Availability Zone.

You can also attach one volume to multiple instances.

EBS Snapshots

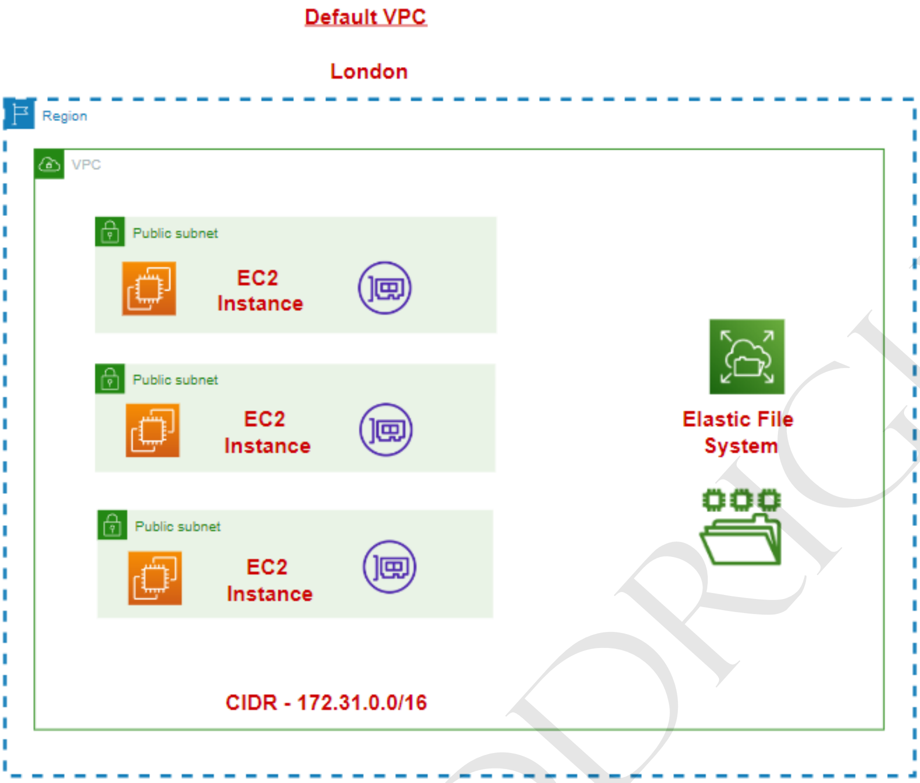


You can take a backup of your data on Amazon EBS volumes to Amazon S3

Here point in time snapshots are taken

The snapshots taken are incremental in nature

Lab - Amazon Elastic File System



Elastic File System allows to create and mount a file system

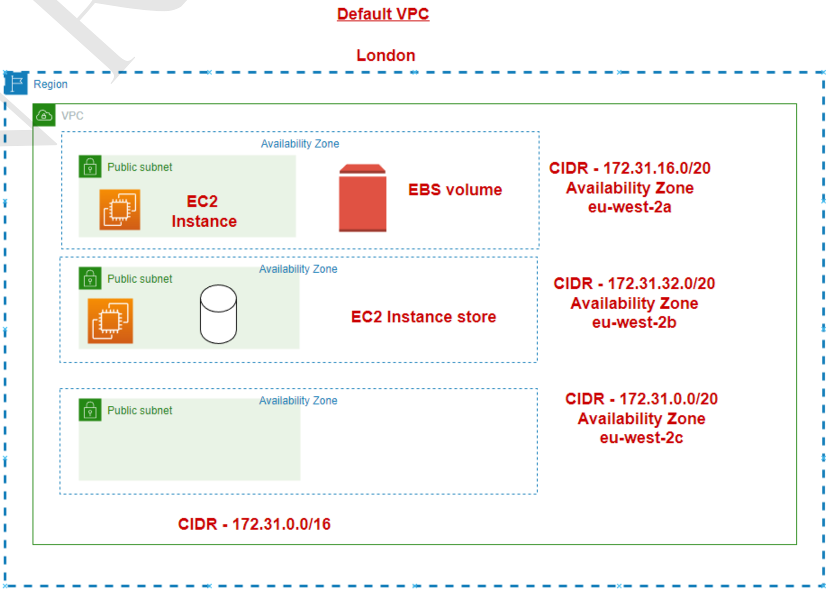
The file system can be shared across resources that include Amazon EC2 instances

Note on EC2 Instance store

This is temporary block-level storage for the instance.

The storage is located on the disks that are physically attached to the host computer.

If you want fast and local storage for the instance.



Amazon S3 service

Amazon S3

This is an object storage service

You can store different types of data here

The storage scale automatically

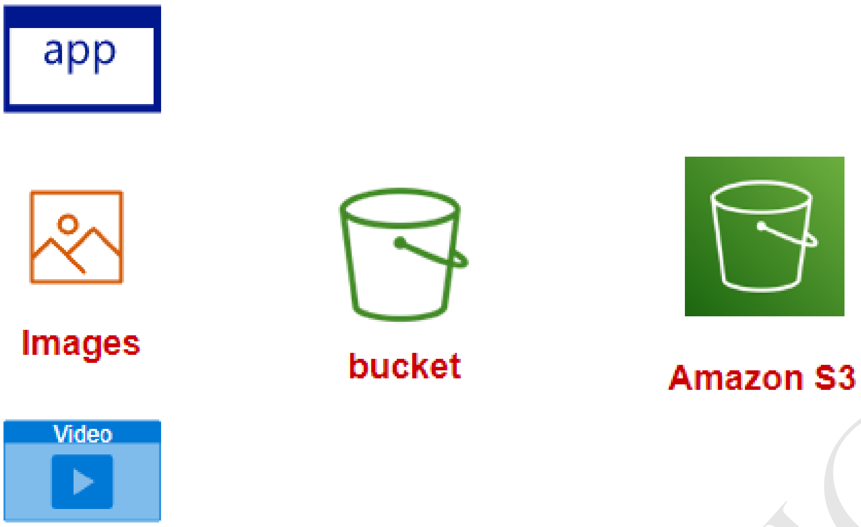
You don't have to worry about the underlying storage

Amazon Simple Storage Service

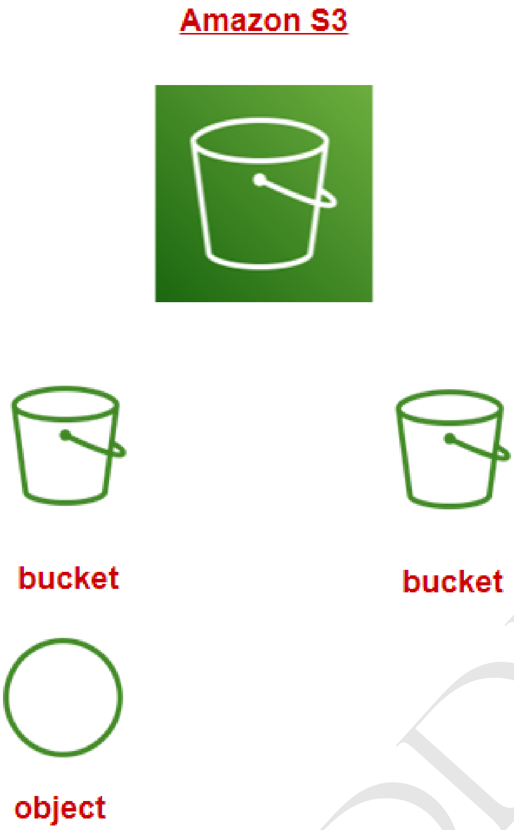
In the service you can create a bucket

The bucket is used to store objects

Each object also gets a unique URL that
can be used to access the object


app
Images
Video
bucket
Amazon S3

Lab - S3 - Object Replication

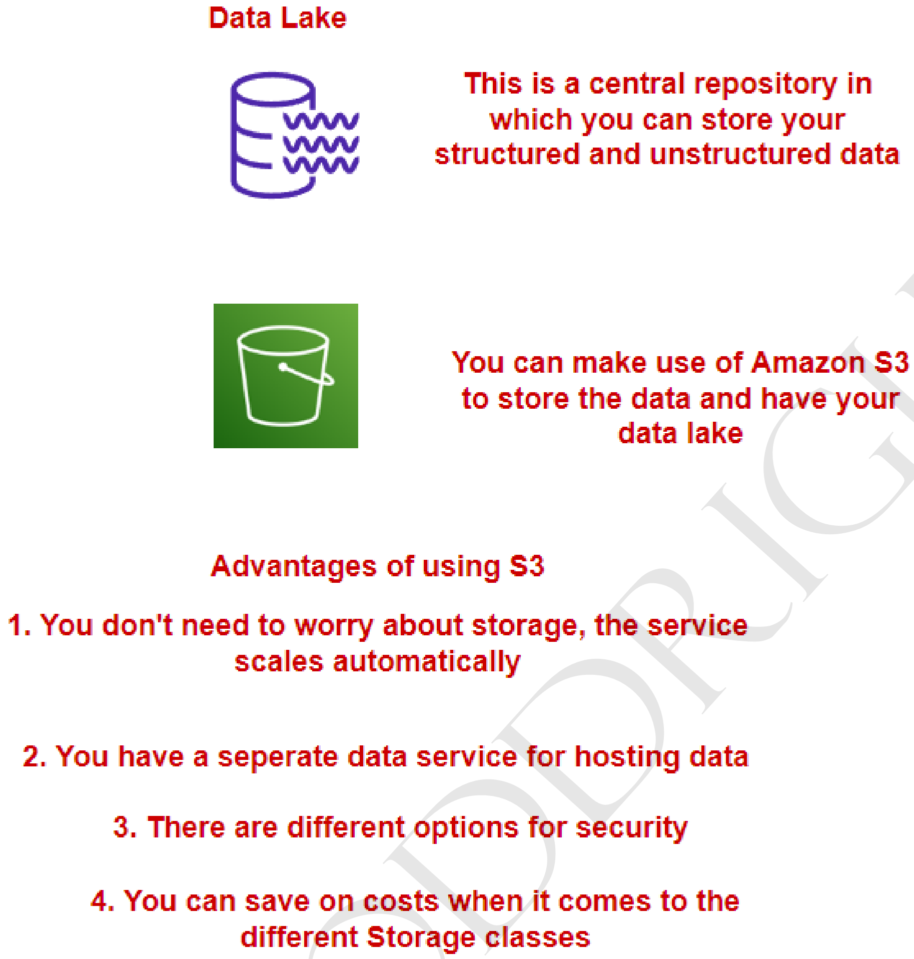


You can enable the replication of objects from one bucket to another

The destination bucket can be in the same or different region.

An IAM role would be created to allow the Amazon S3 service permissions to replicate the objects.

Using Amazon S3 for your data lake



Data Lake

This is a central repository in which you can store your structured and unstructured data

You can make use of Amazon S3 to store the data and have your data lake

Advantages of using S3

1. You don't need to worry about storage, the service scales automatically

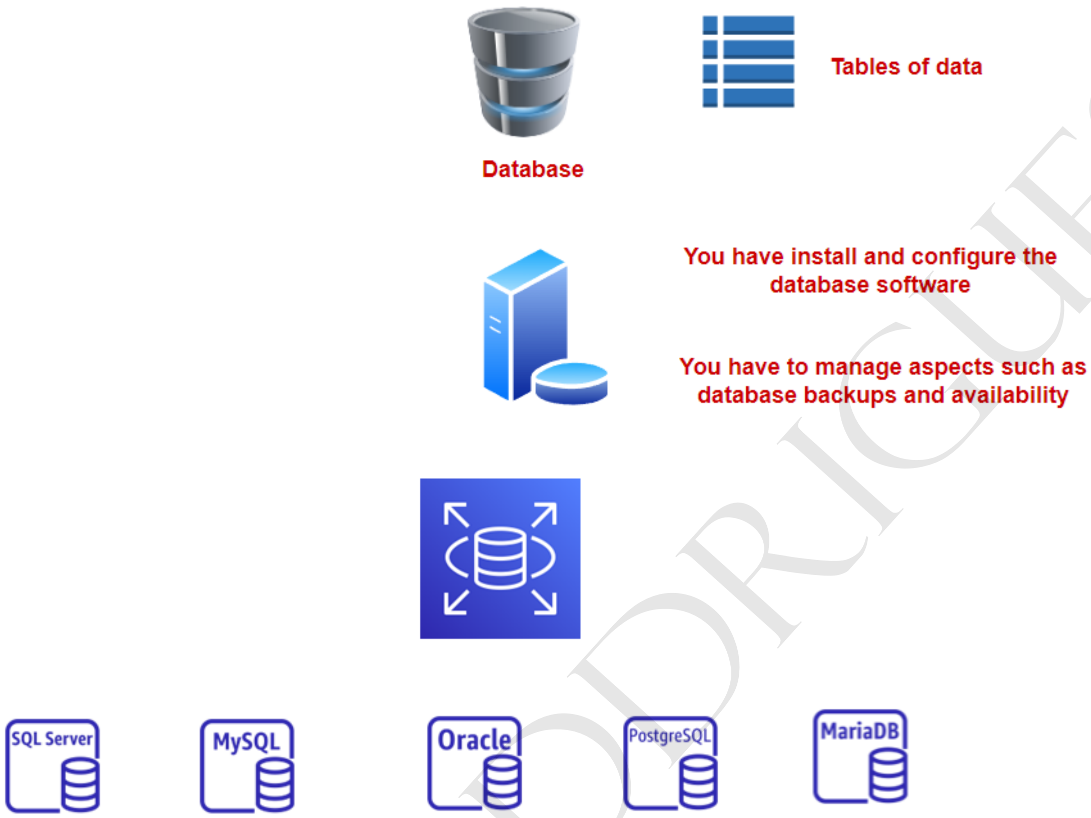
2. You have a seperate data service for hosting data

3. There are different options for security

4. You can save on costs when it comes to the different Storage classes

Amazon RDS service

Amazon Relational Database service



Tables of data

You have install and configure the database software

You have to manage aspects such as database backups and availability

Here the underlying database server infrastructure is managed by AWS

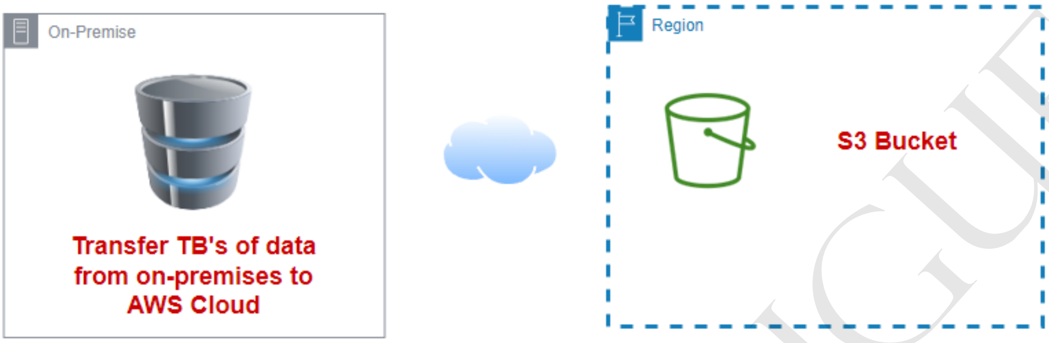
The service also manges backups, software patching, automatic failure detection and recovery

You automatically get high availability as well.

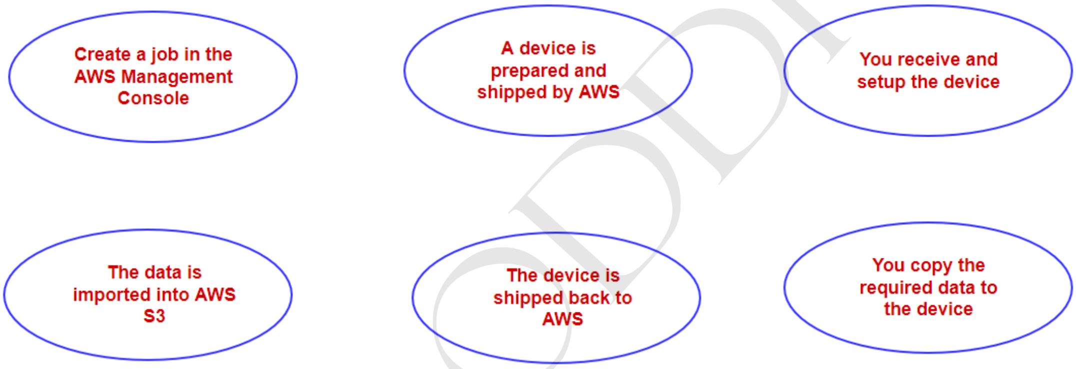
AWS Snowball Edge

AWS Snowball Edge

This can used for transfering data from your on-premises location to AWS



Workflow


Create a job in the AWS Management Console
A device is prepared and shipped by AWS
You receive and setup the device
The data is imported into AWS S3
The device is shipped back to AWS
You copy the required data to the device

Amazon ElastiCache

Amazon ElastiCache

EC2 Instance

Database

Amazon ElastiCache

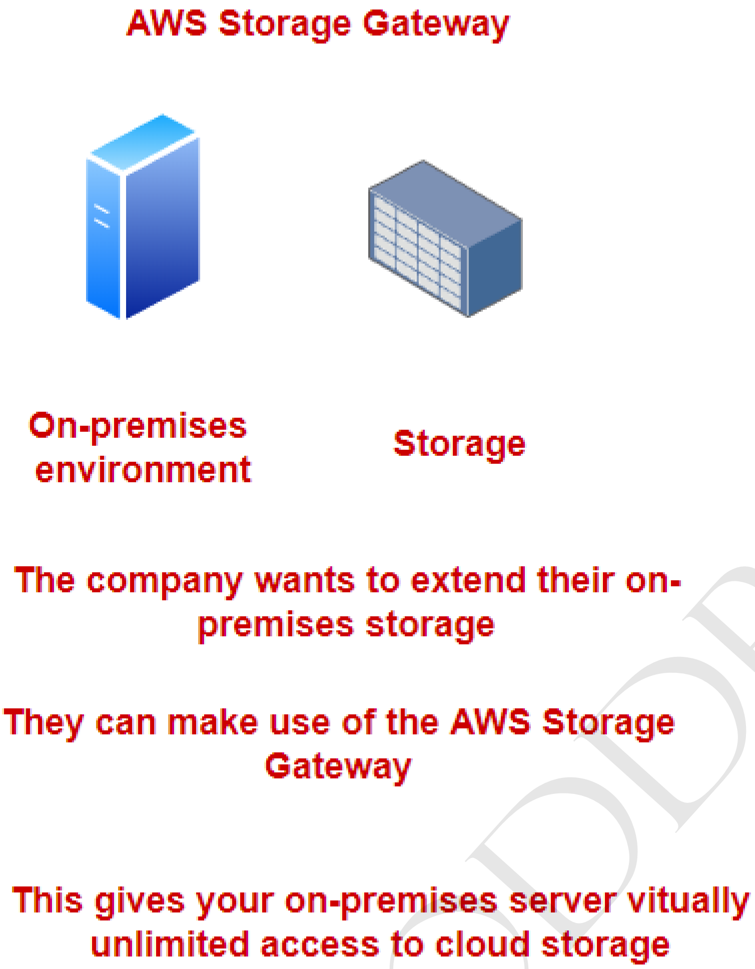
This service helps to easily setup and manage your in-memory data store or cache environment

You have two options - Memcached and Redis

Choose Memcached if you need a simple caching option

The underlying nodes for hosting the cache is completely managed by the service

AWS Storage Gateway



AWS Storage Gateway

On-premises environment

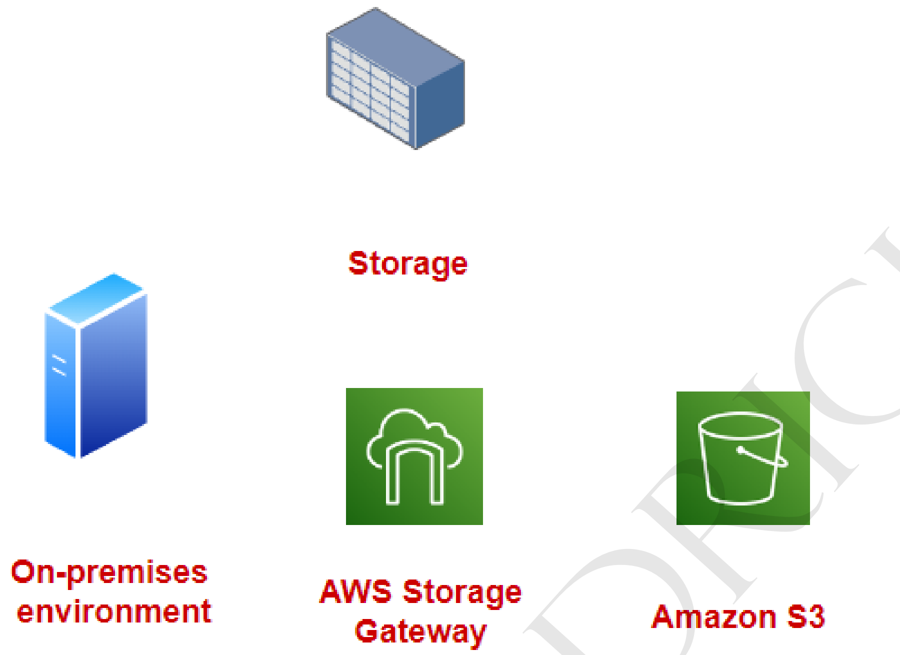
Storage

The company wants to extend their on-premises storage

They can make use of the AWS Storage Gateway

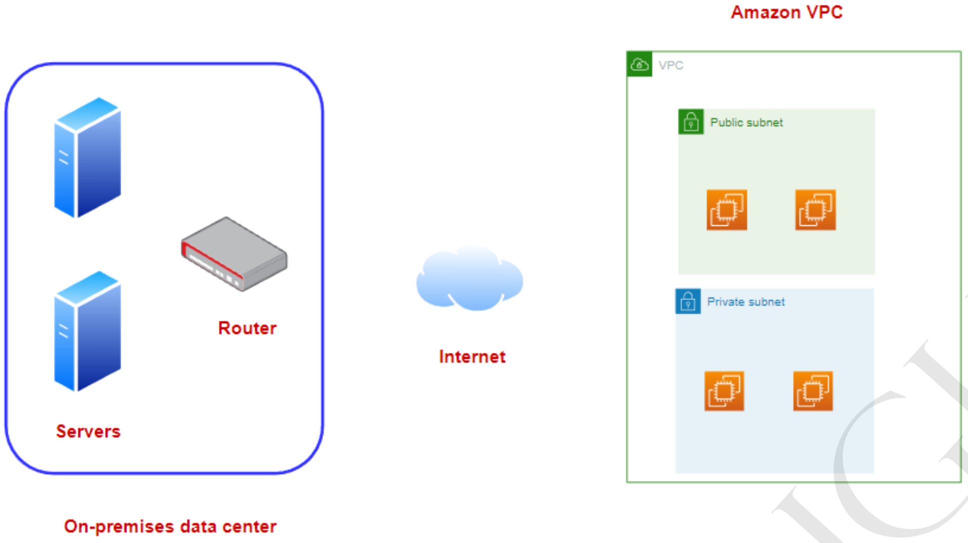
This gives your on-premises server vitually unlimited access to cloud storage

Amazon S3 File Gateway

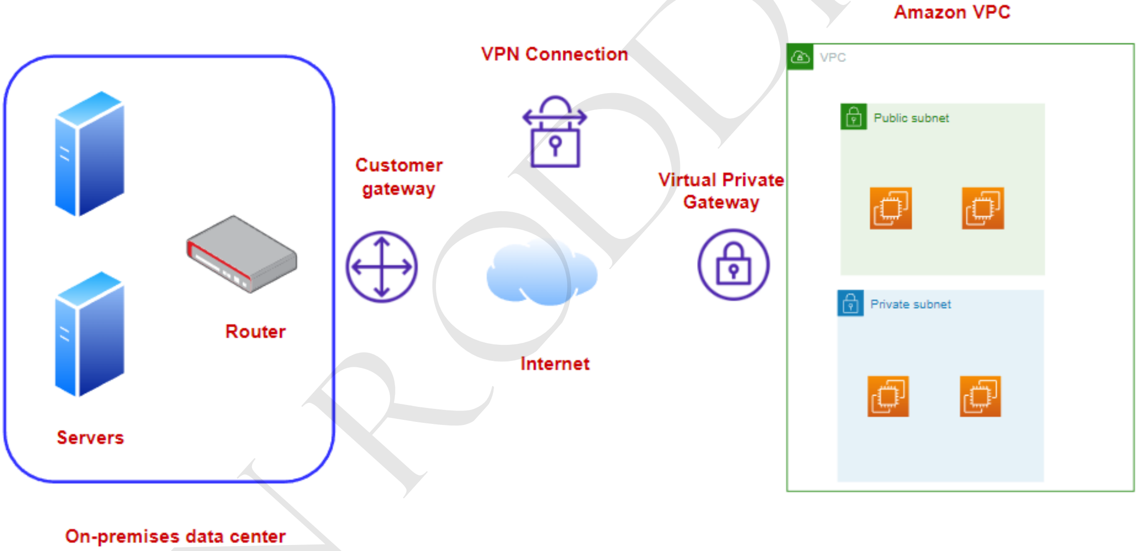


Here the objects stored in S3 are made available to your on-premises servers in the form of files. Clients can connect to S3 via the Network File System(NFS) or Server Message Block(SMB)

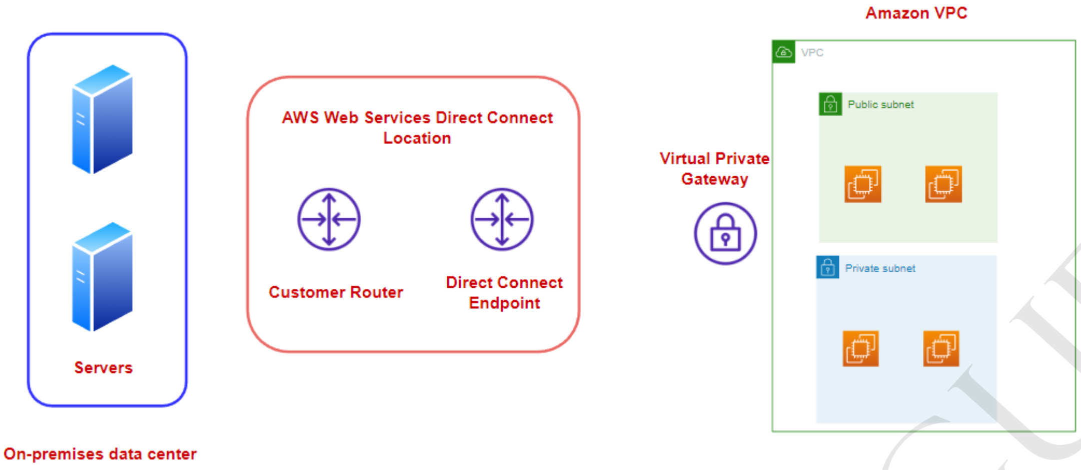
Connecting on-premises network to a VPC



You want to have a secure communication over the Internet between your on-premises data center and the AWS VPC

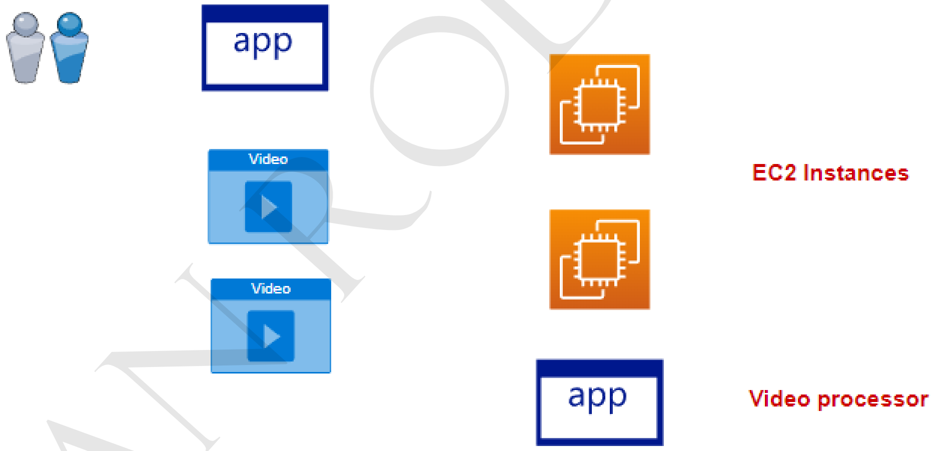


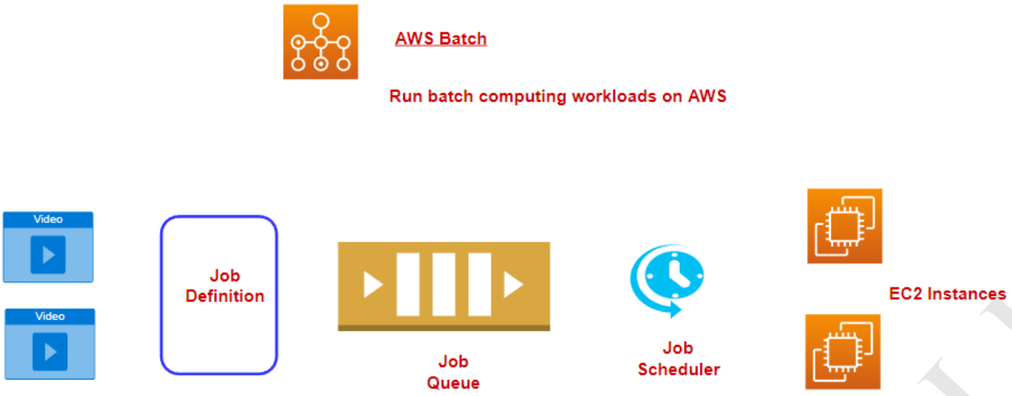
The traffic in the AWS VPN connection is encrypted and hence secure



Here you have a dedicated connection via a Direct Connection Location to AWS

AWS Batch





Lab - AWS Lambda

AWS Lambda

This lets you run code on the cloud without the need of managing servers

app

Code

.NET

Java

Python

EC2 Instance

Install the language runtime

And then run the code

AWS Lambda

You can run code on the cloud without the need of spinning up servers.

AWS Lambda runs your code on high-available compute infrastructure. Manages the capacity and scaling.

Has support for a variety of programming language runtimes - Python, Ruby, Java, Go, C#, PowerShell

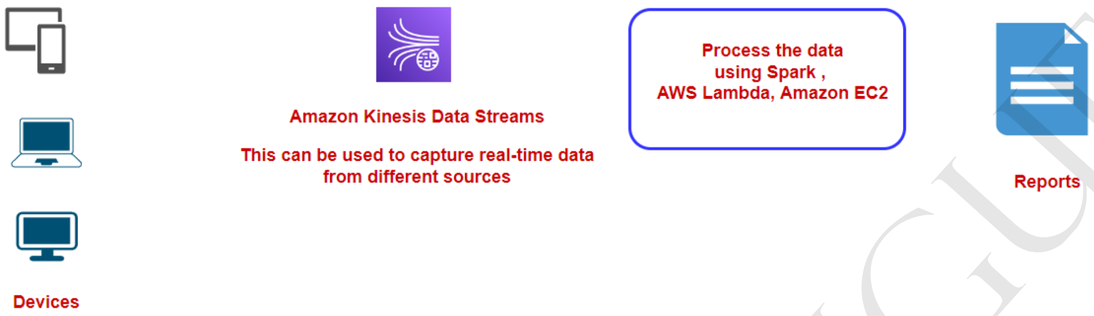
You only pay for the compute time you use

Amazon Kinesis

Amazon Kinesis

Used to collect , process and analyze real-time and streaming data

It can be used to ingest data in real time, like your videos, audio file, log data

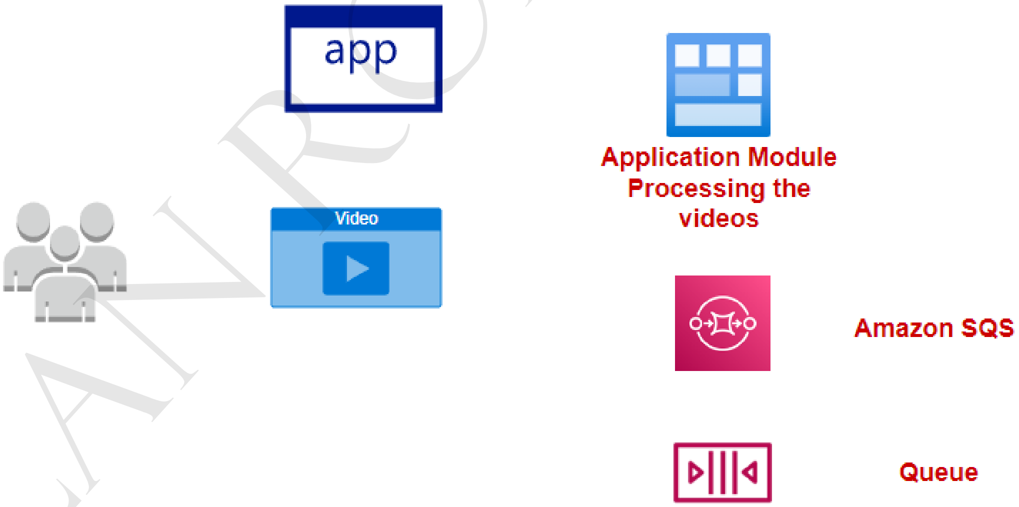

Devices
Amazon Kinesis Data Streams
This can be used to capture real-time data from different sources
Process the data using Spark , AWS Lambda, Amazon EC2
Reports

Lab - Amazon SQS

Amazon Simple Queue Service

This is a messaging service that is fully managed

Helps you decouple distributed software systems and components

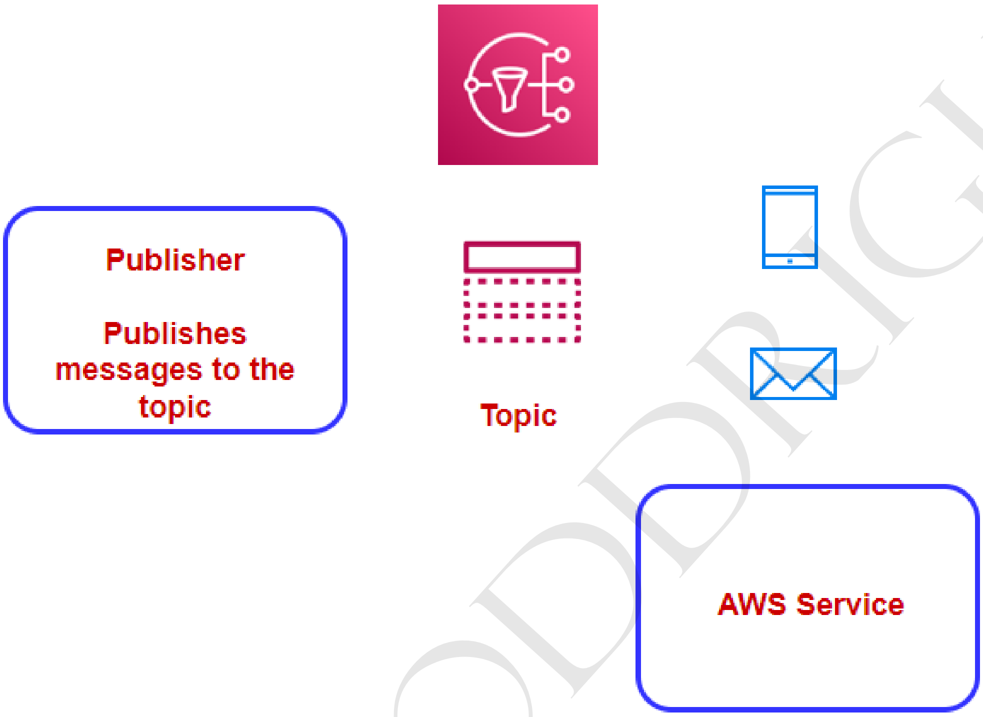


Lab - Amazon SNS

Amazon SNS

This is a message delivery service

Here messages can be delivered to clients that subscribe to a topic



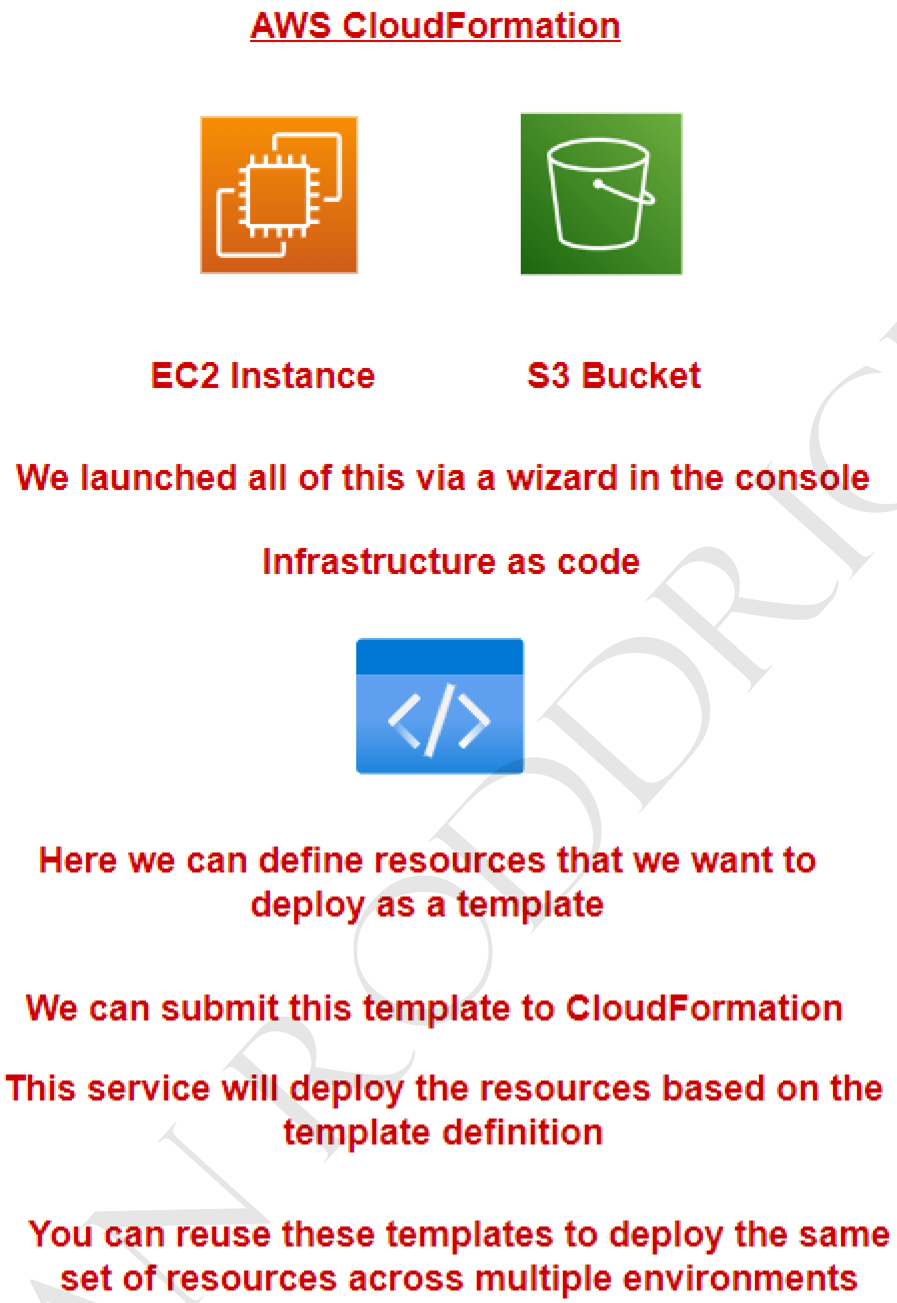
Publisher

Publishes messages to the topic

Topic

AWS Service

Lab - AWS CloudFormation



AWS CloudFormation

EC2 Instance **S3 Bucket**

We launched all of this via a wizard in the console

Infrastructure as code

Here we can define resources that we want to deploy as a template

We can submit this template to CloudFormation

This service will deploy the resources based on the template definition

You can reuse these templates to deploy the same set of resources across multiple environments

About the AWS DevOps set of tools

AWS CodeCommit

1. This is a source control service that can be used to host private Git repositories

2. This is completed managed service

3. Here the code repositories are encrypted at rest and in transit

AWS CodeBuild

1. This service can be used to compile your source code, run unit tests and produce the binaries that are ready to be deployed

2. This is completed managed service

3. It already comes pre-packaged with a host of build environments

AWS CodeDeploy

1. This service can be used to deploy your application components to Amazon EC2 Instances, on-premises servers , AWS Lambda.

2. It can pick up code from a variety of locations for application deployment

3. You can manually stop deployments or roll back deployments

AWS CodePipeline

1. You can automate your entire release process

2. You can create a consistent release process for your application

3. It becomes easier to deploy newer features of your application

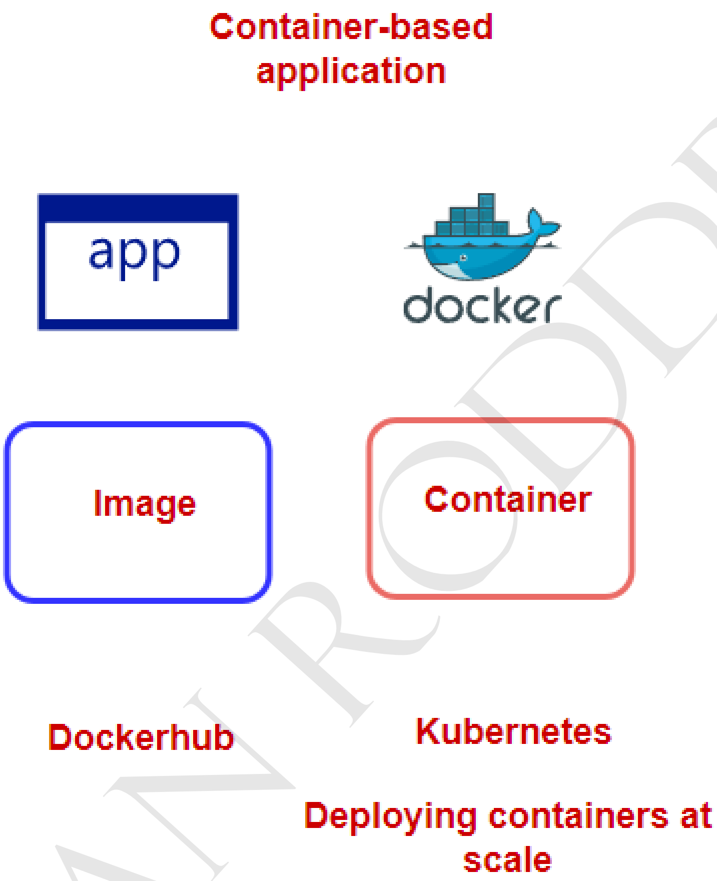
AWS CodeArtifact

1. This is used for storage and sharing of software packages

2. It work seamless with popular package management solutions like NuGet, Maven, Gradle etc.

3. Your developers can then consume the packages from within AWS CodeArtifact

AWS Tools for containers



Container-based application

Image

Container

Dockerhub

Kubernetes

Deploying containers at scale

Amazon Elastic
Container Registry

1. This is an image registry service

2. You can push your container images to the repository

3. The service is secure and scalable

Amazon Elastic Container Service

1. This is a container management service

2. Here your containers run in a cluster

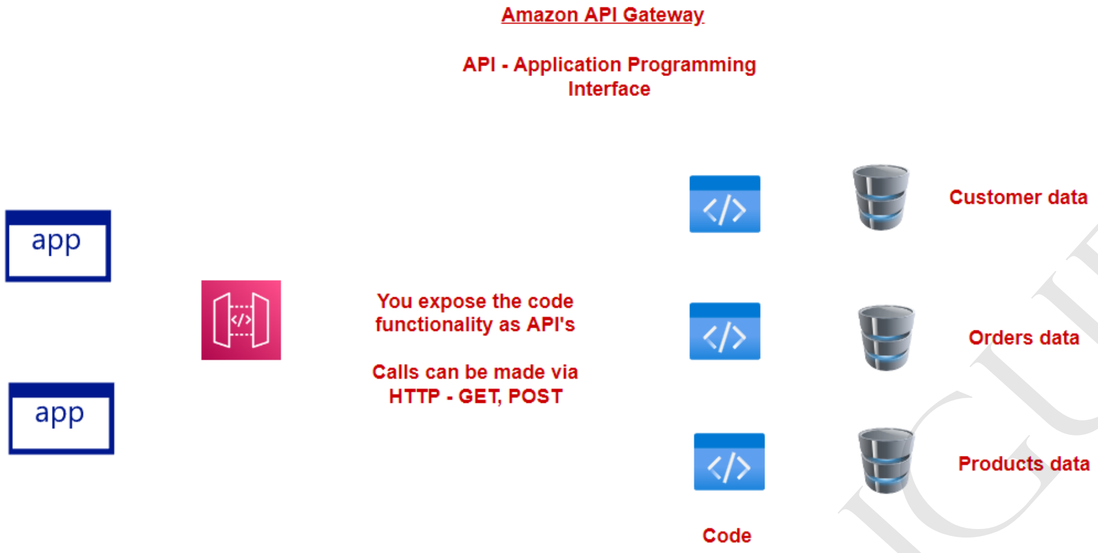
3. This is normally the service of choice when it comes Microservice architectures

AWS Fargate

1. This is a serverless option when it comes a container management service.

2. Here all of the infrastructure is managed for you.

Amazon API Gateway



Amazon API Gateway

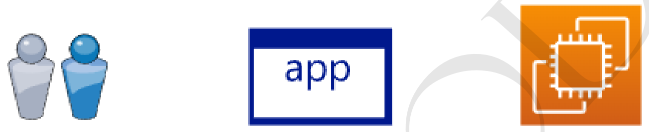
API - Application Programming Interface

You expose the code functionality as API's

Calls can be made via HTTP - GET, POST

AWS Elastic Load Balancer

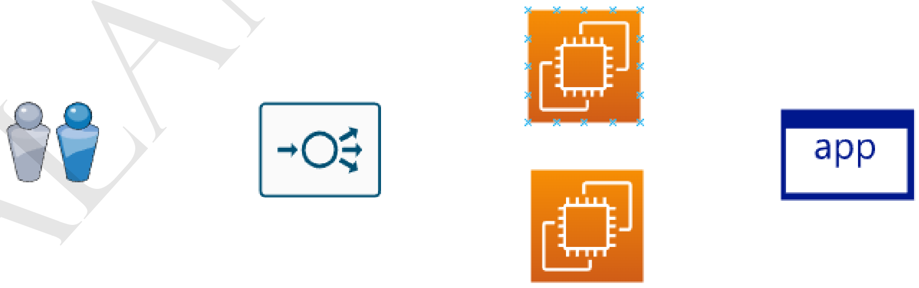
Load Balancer



EC2 Instance

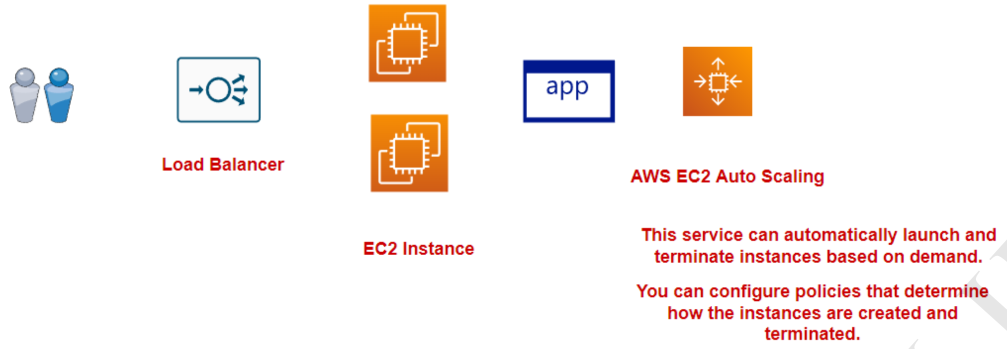
CPU, RAM

You can scale vertically by adding more CPU and RAM



EC2 Instance

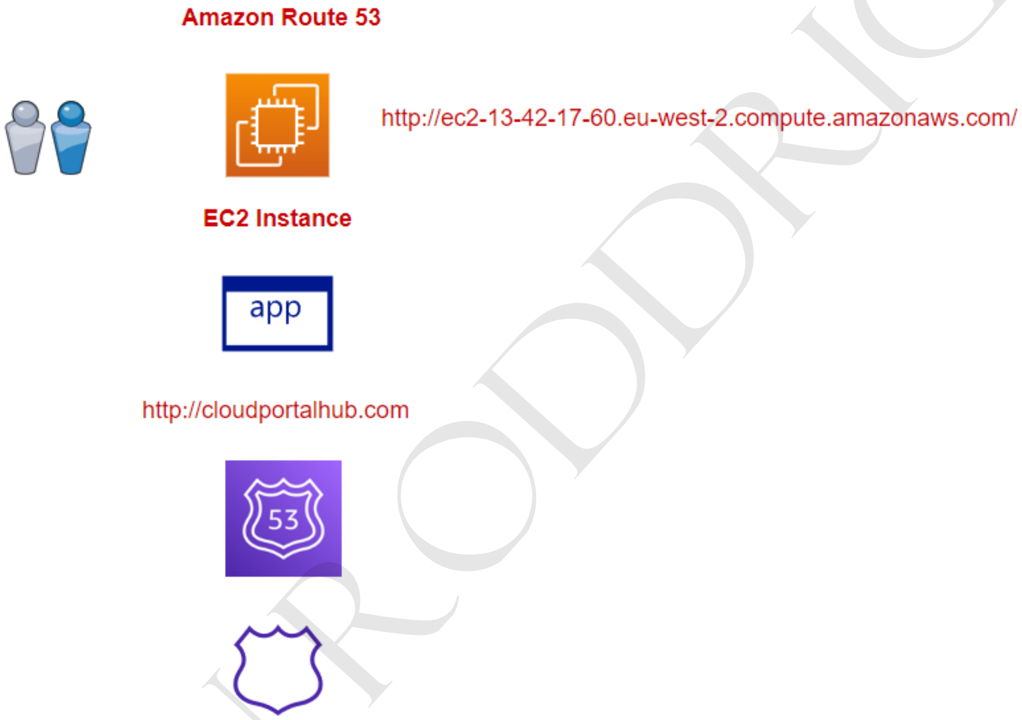
Lab - Amazon EC2 Auto-Scaling Groups



This service can automatically launch and terminate instances based on demand.

You can configure policies that determine how the instances are created and terminated.

Amazon Route 53

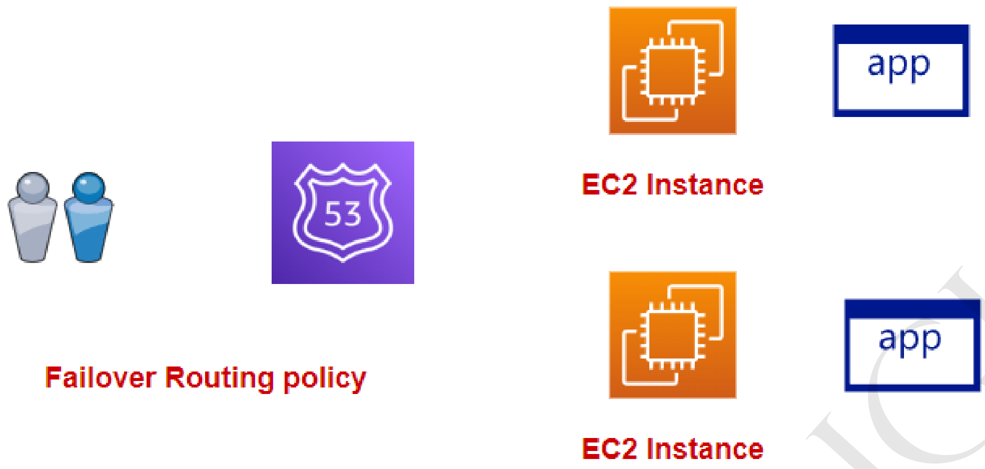

Amazon Route 53
http://ec2-13-42-17-60.eu-west-2.compute.amazonaws.com/
EC2 Instance
app
http://cloudportalhub.com
53
Public Hosted Zone

The public hosted zone has records on how to route traffic to the domain

We create an A record. We can use that A record to point our domain traffic to an EC2 Instance

Amazon Route 53 - Routing policies

Amazon Route 53 Routing policies

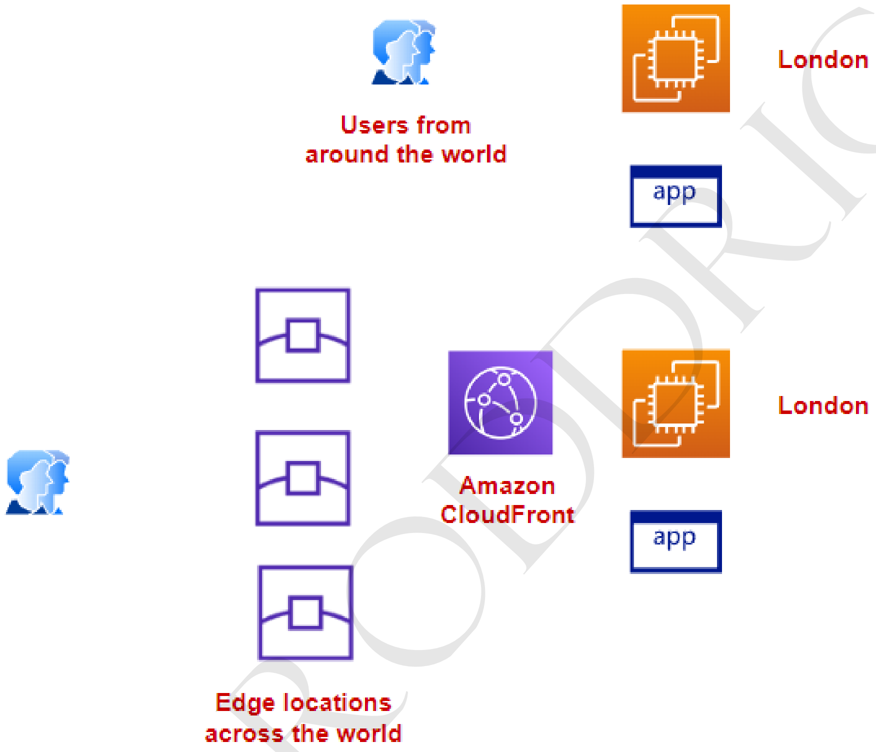


Amazon CloudFront

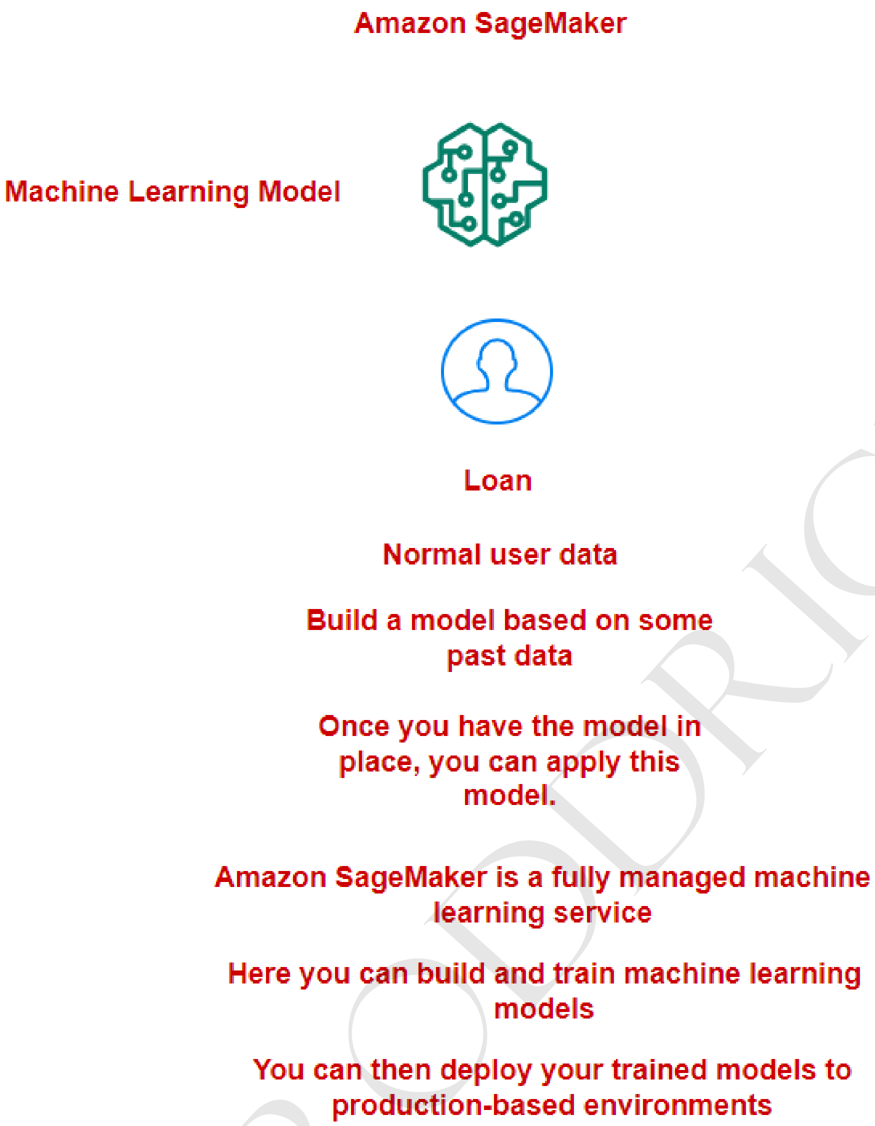
Amazon CloudFront

This service can be used to speed up the distribution of static and dynamic web content

When a user requests for content via CloudFront, the request is routed to an edge location that can provide the least latency.



Amazon SageMaker



Amazon SageMaker

Machine Learning Model

Loan

Normal user data

Build a model based on some past data

Once you have the model in place, you can apply this model.

Amazon SageMaker is a fully managed machine learning service

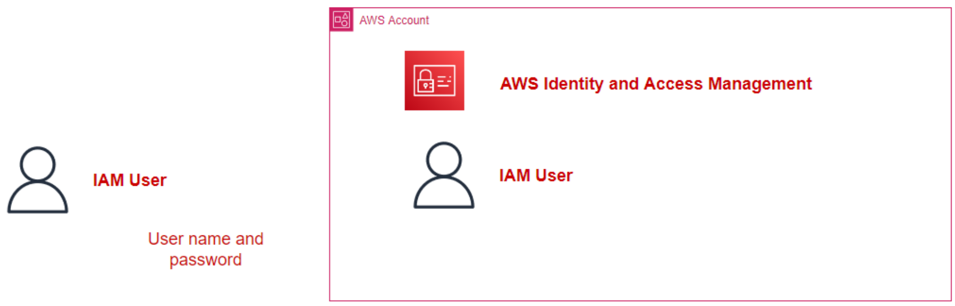
Here you can build and train machine learning models

You can then deploy your trained models to production-based environments

Domain - Security and Compliance

AWS Multi-Factor Authentication

Multi-Factor Authentication



The use of MFA - Multi-Factor Authentication to provide an extra layer of security when it comes to authentication

Virtual MFA devices - This is a software that runs on a phone or another device

Hardware MFA device - This generates a numeric code that the user can use to log into the account

FIDO security key - This is a device that can plug into your computer that can be used in the authentication process.

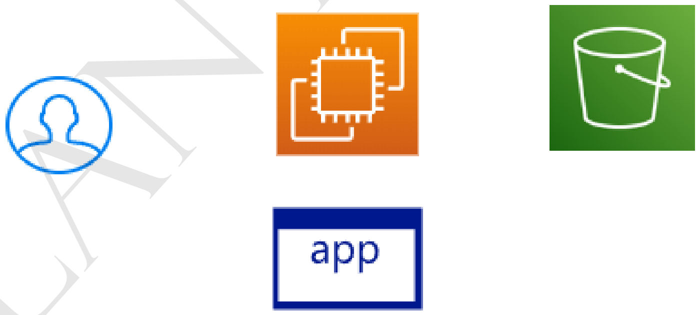
IAM Roles

IAM Roles

This is an identity that is created that is given specific permissions

Here the role can be assumed by anyone who requires it

The entity can assume the role and then based on the permissions granted can perform the required operations



IAM user

Give the user access to the S3 bucket

Embed the AWS access keys in the application

But there is a more secure way to accomplish this

Create an IAM Role that can be attached to the EC2 instance

This role has the permissions to access the S3 bucket

Shared Responsibility Model

EC2 Instance

AWS is responsible for the uptime of the service

Customer is responsible for the applications and data on the EC2 Instance

The installation of security updates and patches at the OS level is the responsibility of the customer

The installation of security updates and patches at the hardware level is the responsibility of AWS

Shared Control

The configuration of services at OS level is the responsibility of the customer

The configuration at the hardware level is the responsibility of AWS

Shared Control

AWS provides training to their staff

The company needs to provide training to their staff

Shared Control

EC2 Instance

AWS Responsibility

Install the latest security updates on the physical server

Uptime of the underlying physical infrastructure

Latest AMI's are available

Customer Responsibility

Install the latest security updates on the EC2 Instance when it comes to the OS and applications

Protect the data hosted on the EC2 Instance

Protect the data hosted on the EC2 Instance

Protect the application hosted on the EC2 Instance

AWS Lambda

AWS Responsibility

Ensure the latest runtime is available for the programming language

Manage the physical infrastructure

Customer Responsibility

Configure and maintain the Lambda function

Hosting a database

AWS RDS

AWS Responsibility

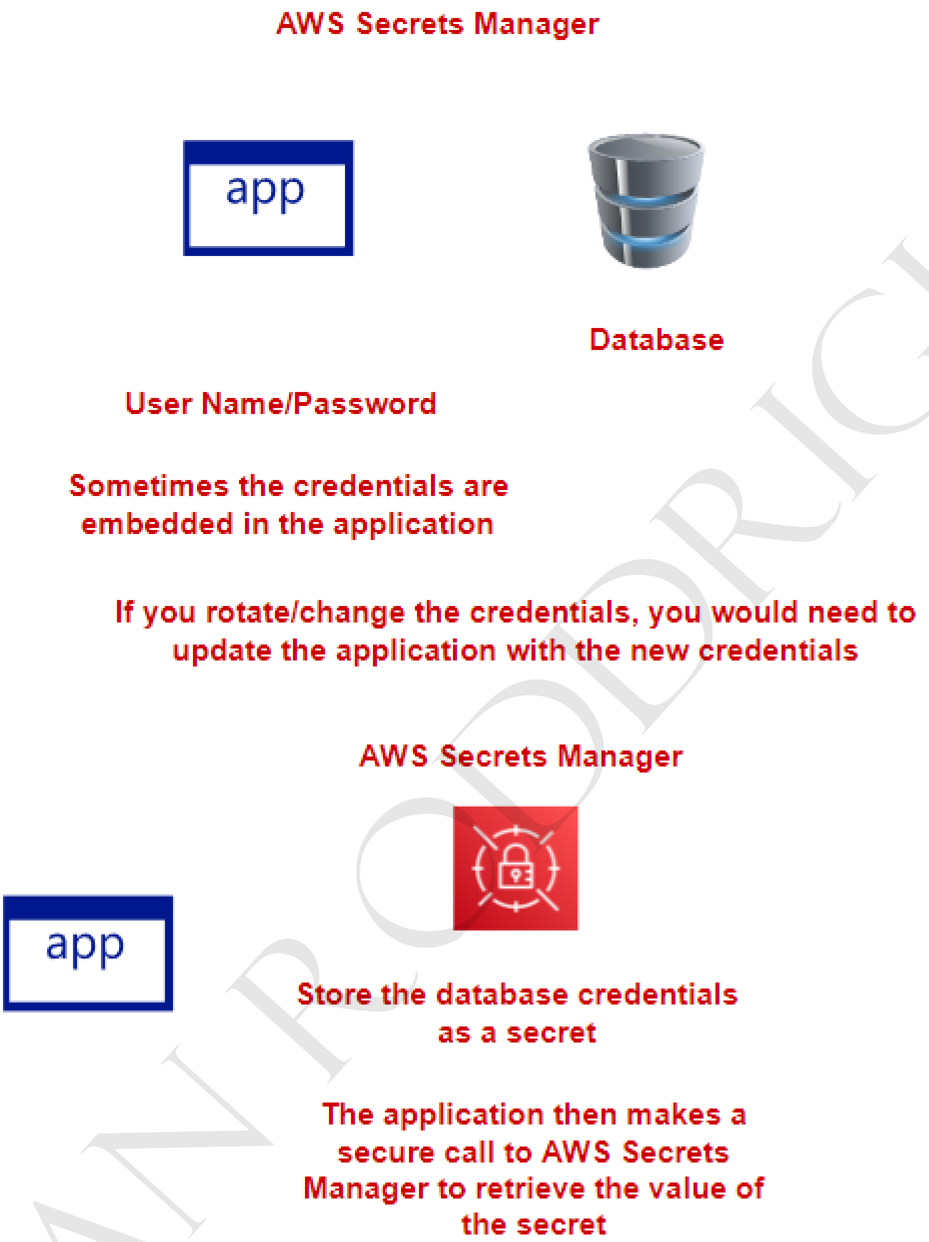
Uptime of the Amazon RDS service

Patching of the compute infrastructure and the database engine

Customer Responsibility

Responsible for data

AWS Secrets Manager



AWS Secrets Manager

Database

User Name/Password

Sometimes the credentials are embedded in the application

If you rotate/change the credentials, you would need to update the application with the new credentials

AWS Secrets Manager

Store the database credentials as a secret

The application then makes a secure call to AWS Secrets Manager to retrieve the value of the secret

AWS Certificate Manager

Browser

Server

Employ the use of SSL certificates

This is a digital certificate that can be used to authenticate a website's identity.

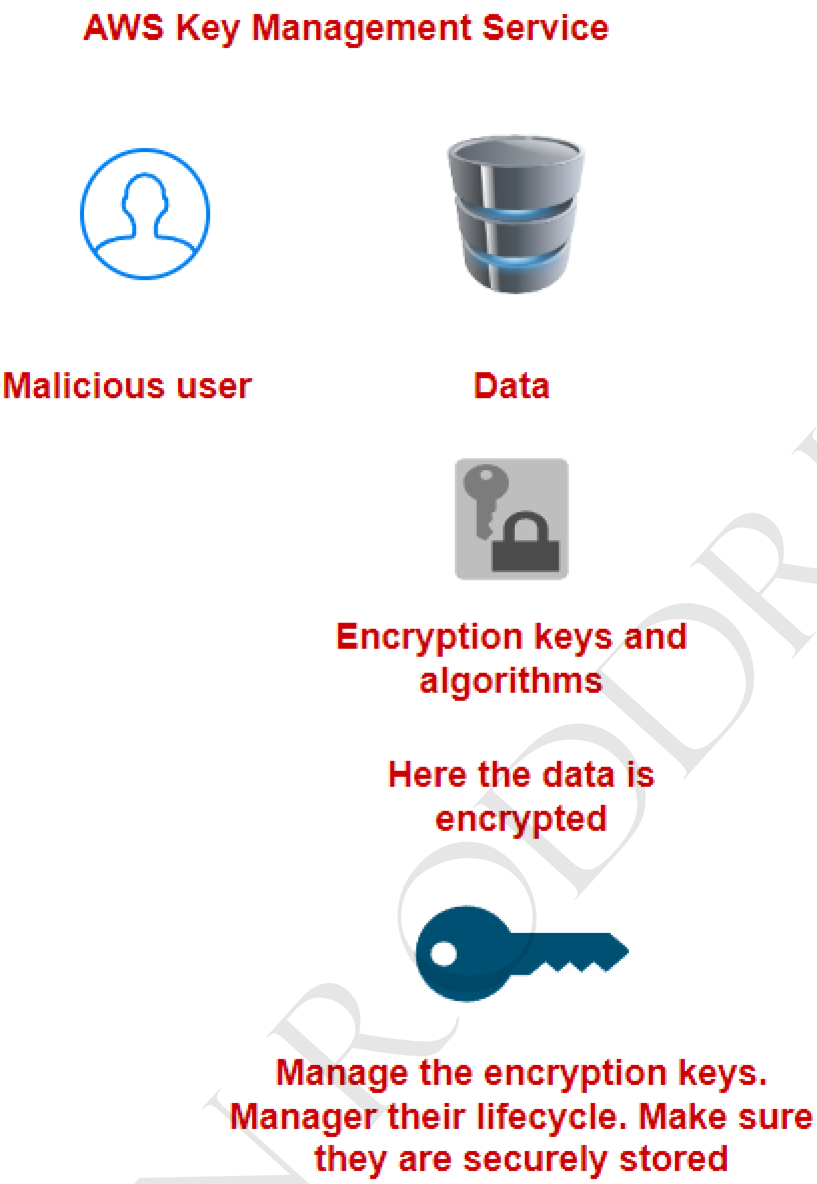
It also helps to create a secure connection between the web server and the browser application

AWS Certificate Manager

This service can be used for creating, storing and renewing your public and private certificates

You can also import third-party certificates

The AWS Certificate Manager also integrates with AWS service such as the Elastic Load Balancer and Amazon CloudFront



AWS Key Management Service

Malicious user

Data

Encryption keys and algorithms

Here the data is encrypted

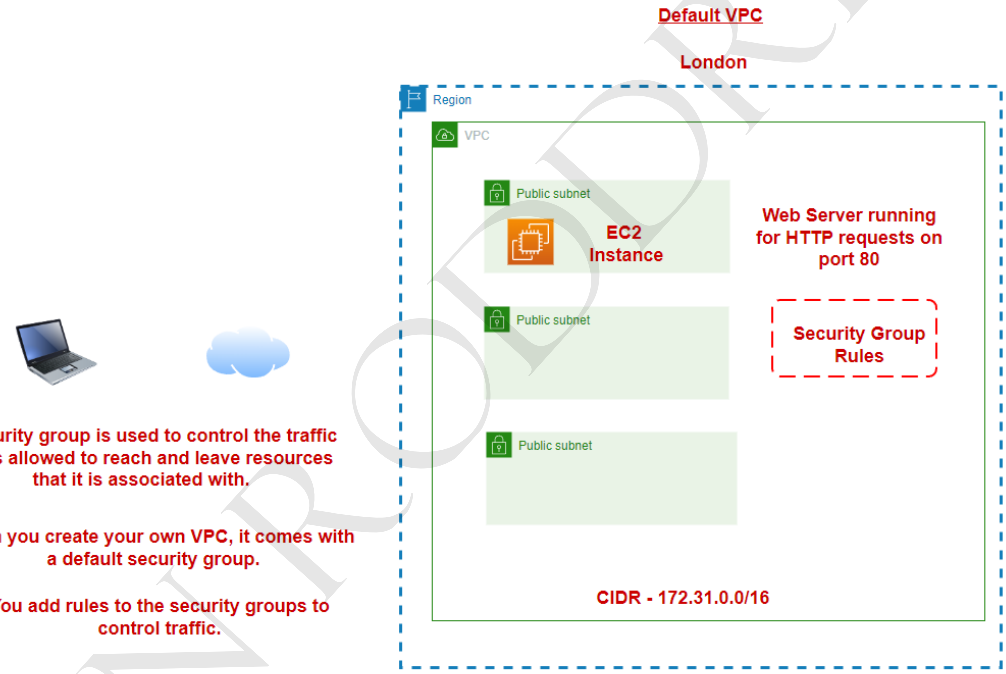
Manage the encryption keys. Manager their lifecycle. Make sure they are securely stored

AWS Key Management Service

This is a managed service that can be used to create and control the use of cryptographic keys.

These keys can then be used to protect your data.

AWS Security Groups

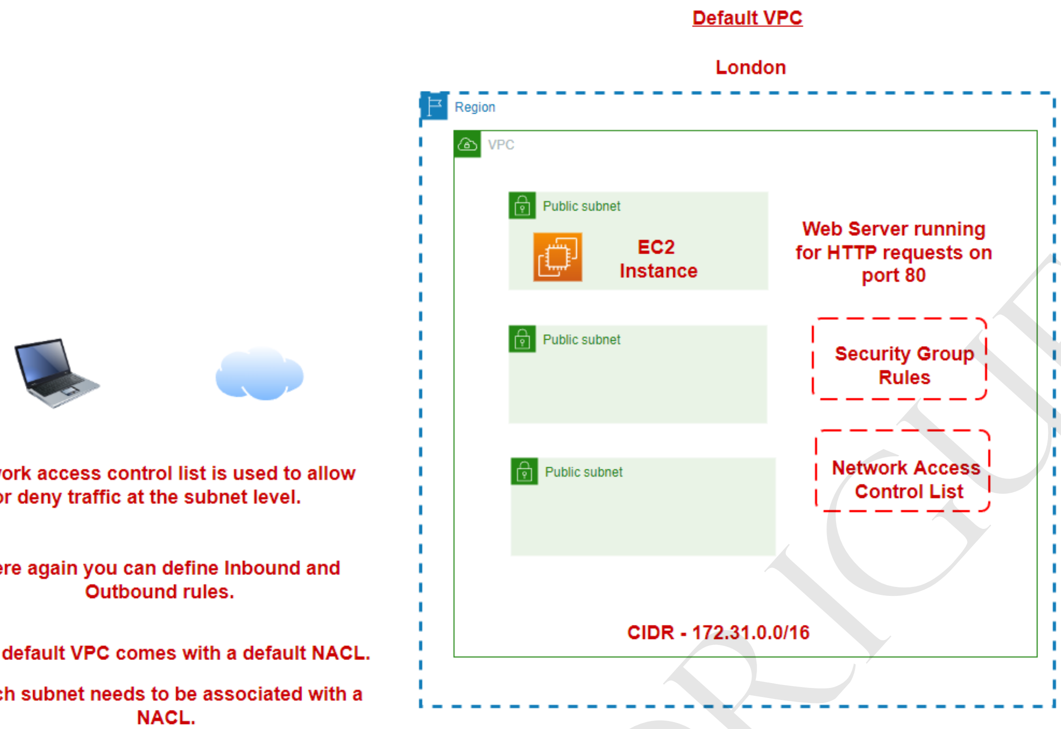


A security group is used to control the traffic that is allowed to reach and leave resources that it is associated with.

When you create your own VPC, it comes with a default security group.

You add rules to the security groups to control traffic.

Network Access Control Lists



A network access control list is used to allow or deny traffic at the subnet level.

Here again you can define Inbound and Outbound rules.

The default VPC comes with a default NACL.

Each subnet needs to be associated with a NACL.

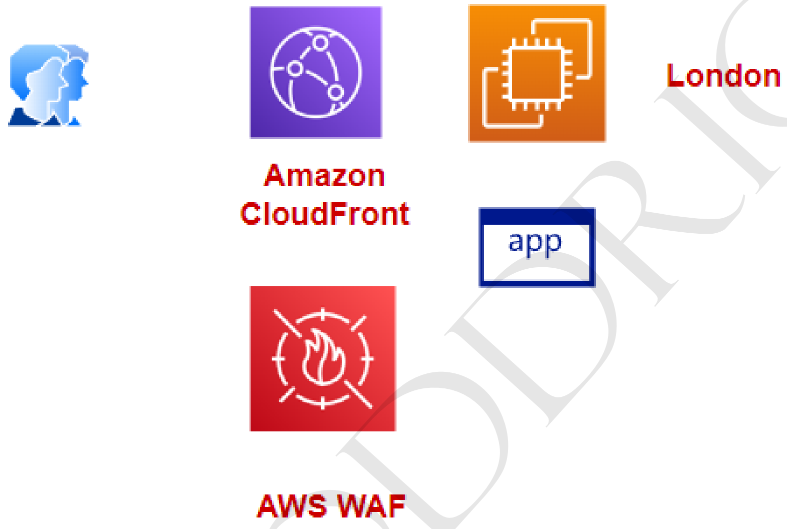
AWS Web Application Firewall

AWS WAF

This is a web application firewall

This is used for protecting your web applications

It can protect against attacks against your web application like SQL injection or cross-site scripting attacks



You can protect resources that include Amazon CloudFront distributions, Amazon API Gateway , Application Load Balancer

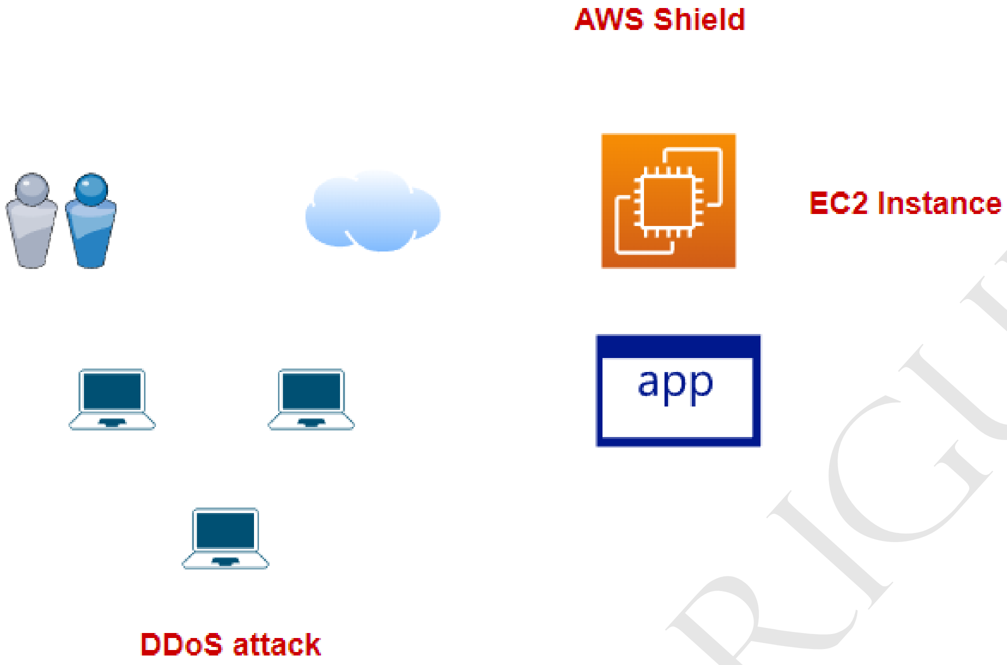
Rules

The rules can perform certain actions based on certain criteria

You can block requests that are based on HTTP headers

If the HTTP headers don't have the appropriate values, then just block the request

AWS Shield



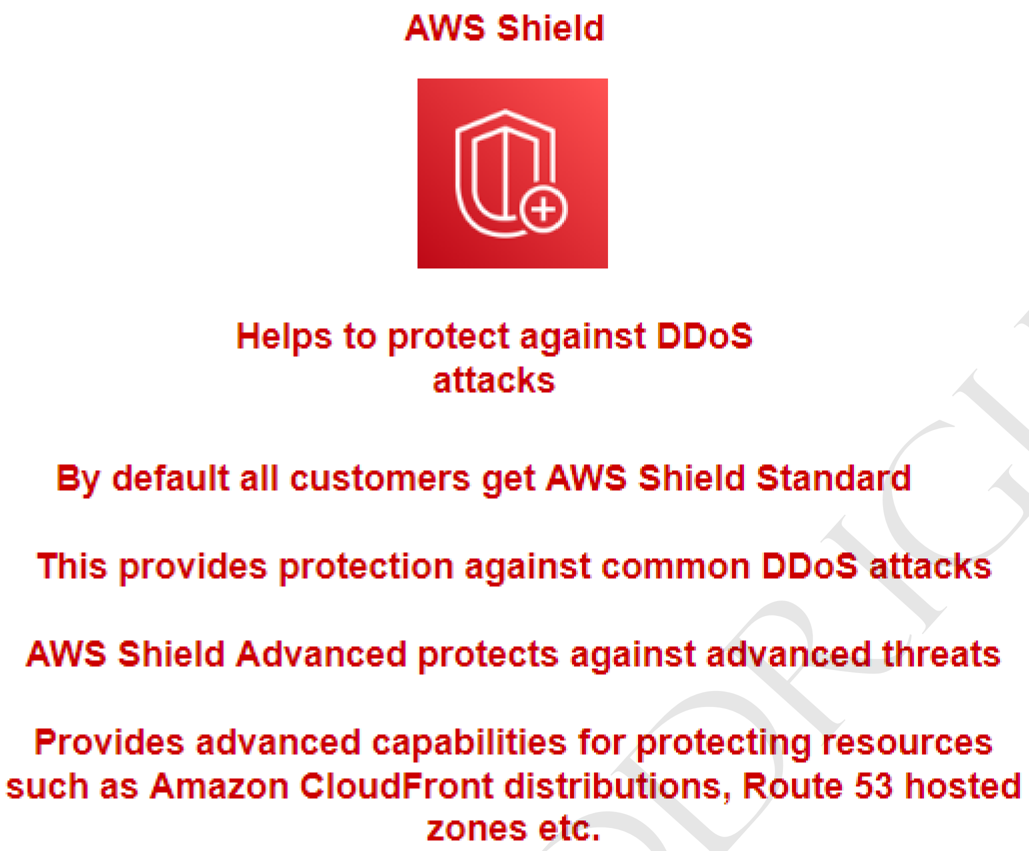
AWS Shield

EC2 Instance

DDoS attack

Distributed Denial of Service

Here the systems are trying to flood the target with traffic



AWS Shield

Helps to protect against DDoS attacks

By default all customers get AWS Shield Standard

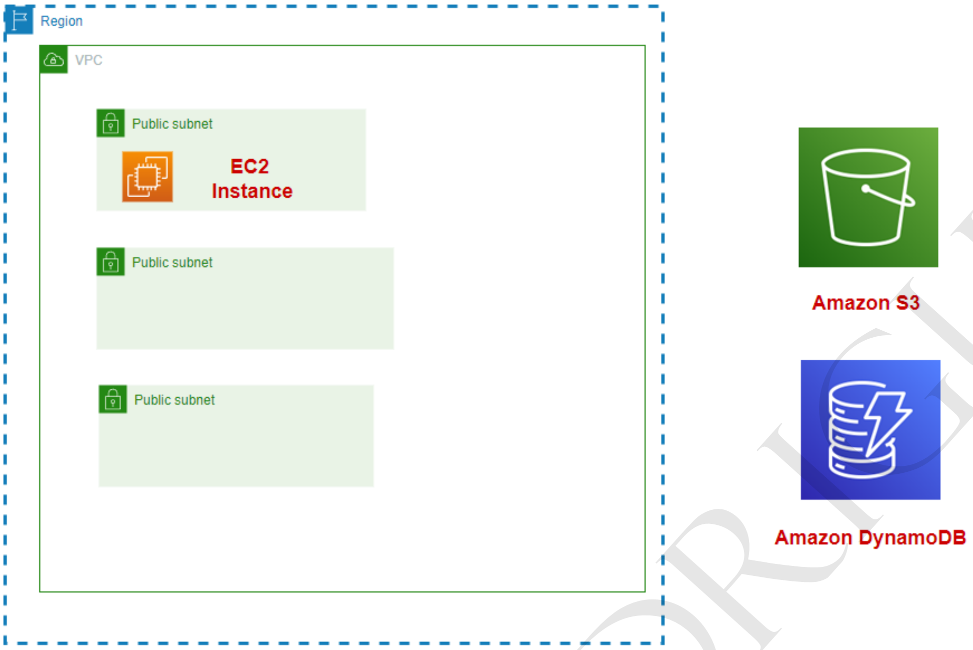
This provides protection against common DDoS attacks

AWS Shield Advanced protects against advanced threats

Provides advanced capabilities for protecting resources such as Amazon CloudFront distributions, Route 53 hosted zones etc.

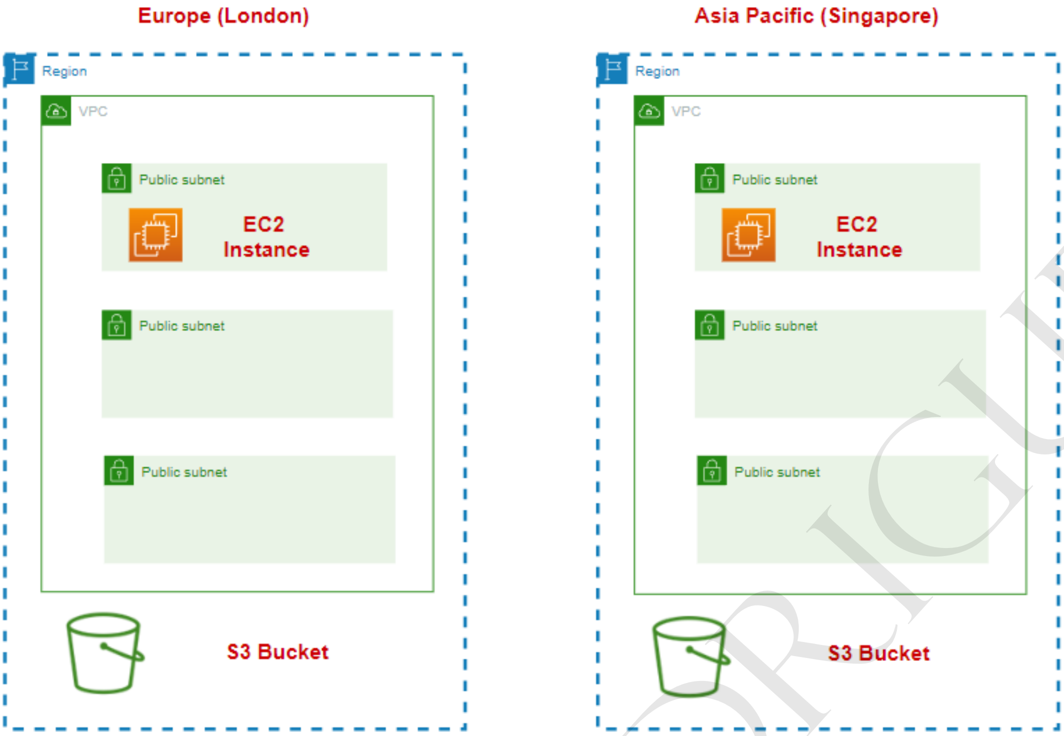
Note on VPC Endpoints

VPC Endpoints provide connectivity to Amazon S3 and DynamoDB without the need of having an Internet Gateway or any sort of NAT device for the VPC



Domain - Cloud Concepts

Taking advantage of AWS regions



Each region is seperate

Pricing is different per region

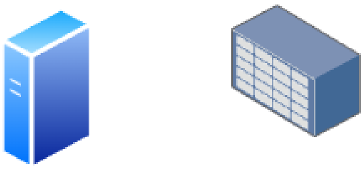
You can easily deploy resources to different regions

You cannot move resources that easily from one region to another

You can use the AWS Console to manage your resources across regions

Advantages of AWS Cloud Computing

1. Trade fixed expenses for variable expenses



Invest in servers and storage

EC2 Instance

EBS Volume

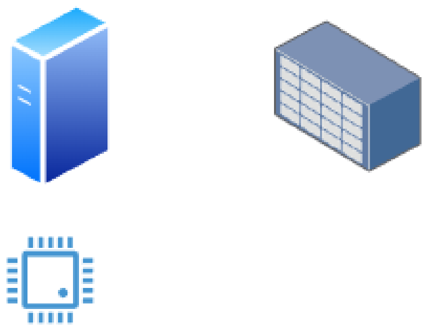
You only pay for how much you use

You can terminate resources whenever they are not required

2. Benefits from massive economies of scale

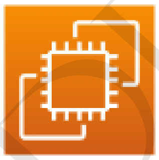
As more and more customer start adopting AWS, AWS can achieve higher economies of scale. And this can lead to lower pay-as-you-go prices

3. Stop guessing capacity



Normally when investing in hardware, you need to know how many CPU's are needed, how many Terabytes of storage are needed

And its difficult to scale whenever required



EC2 Instance

But with AWS resources you can scale whenever required

4. Increase speed and agility

Because of the advantages when it comes to infrastructure, you can focus on delivering newer features for your application.

5. Don't need to spend money maintaining data centers

6. Go global in minutes

You can deploy resources to different regions within no time at all.

Benefits of Cloud Computing – Elasticity

Elasticity

This concept relates to the fact that you can create resources whenever required. And then release the resources when they are not required.

Create an EC2 Instance when required

If the EC2 Instance is not being utilized, delete the resource

The other aspect of Elasticity is having the ability to scale out or scale in based on demand.

Amazon S3 - Here the storage scales on demand

Amazon EC2 Auto Scaling - Scale EC2 Instances on demand

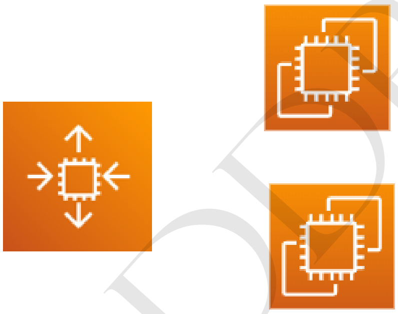
Benefits of Cloud Computing - Scalability

Scalability

Scale based on demand

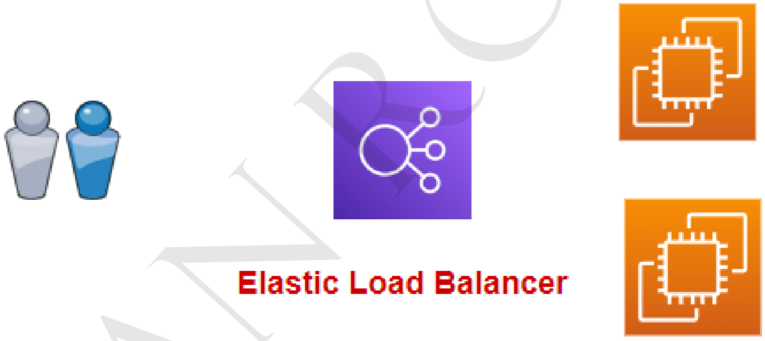
S3 storage

The storage scales in the background



EC2 Auto-scaling group

EC2 Instances



Elastic Load Balancer

EC2 Instances

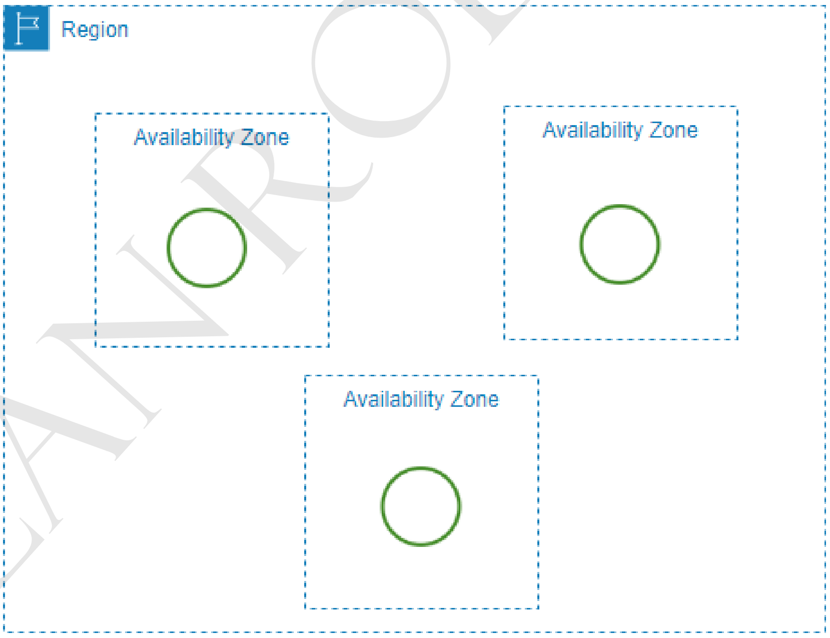
Elastic Load Balancer can scale based on demand

High Availability

As much as possible you want the application infrastructure to be up and running.

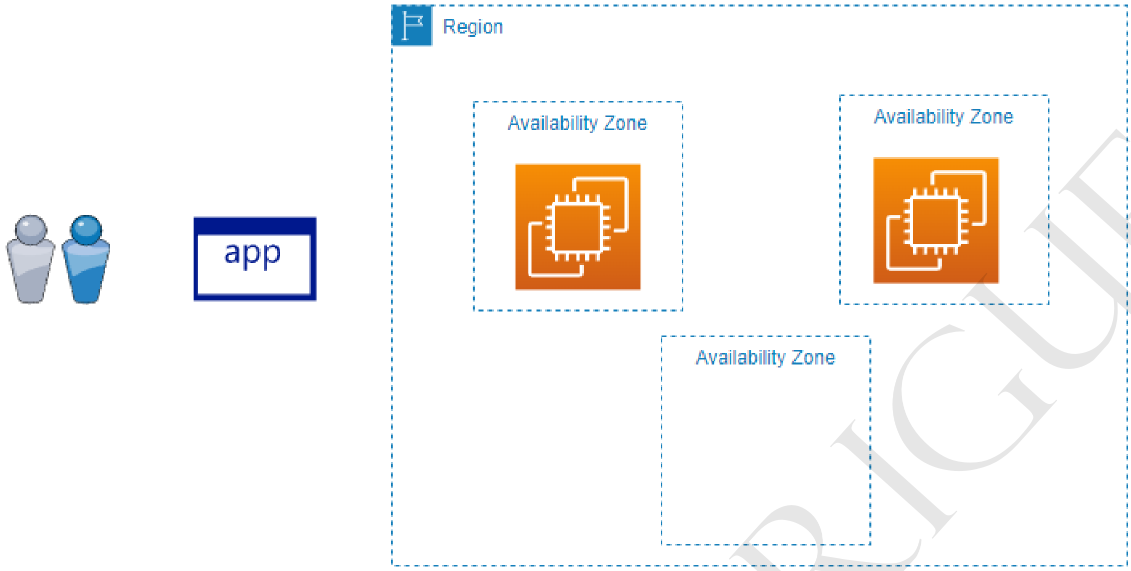
EC2 Instance
S3 bucket
app

The S3 service achieves high durability for your objects for most of the storage classes

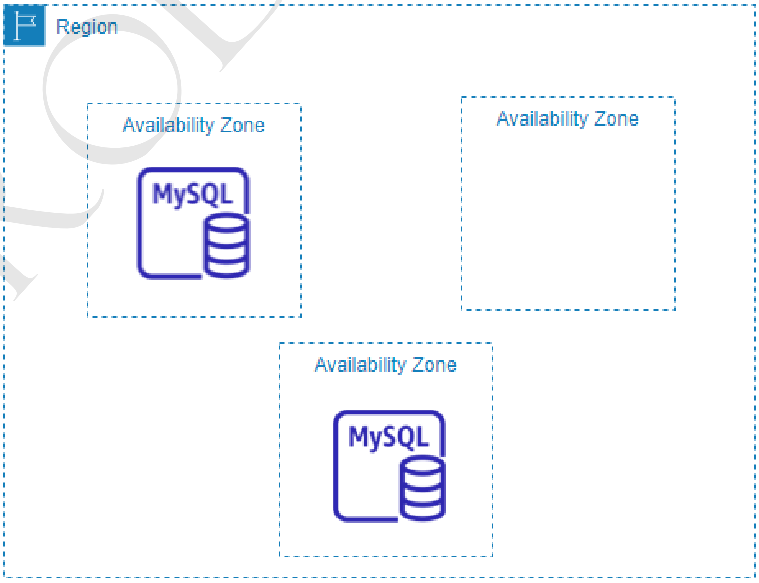


The S3 service by default copies the object on multiple devices across a minimum of three Availability Zones.

For your EC2 Instance

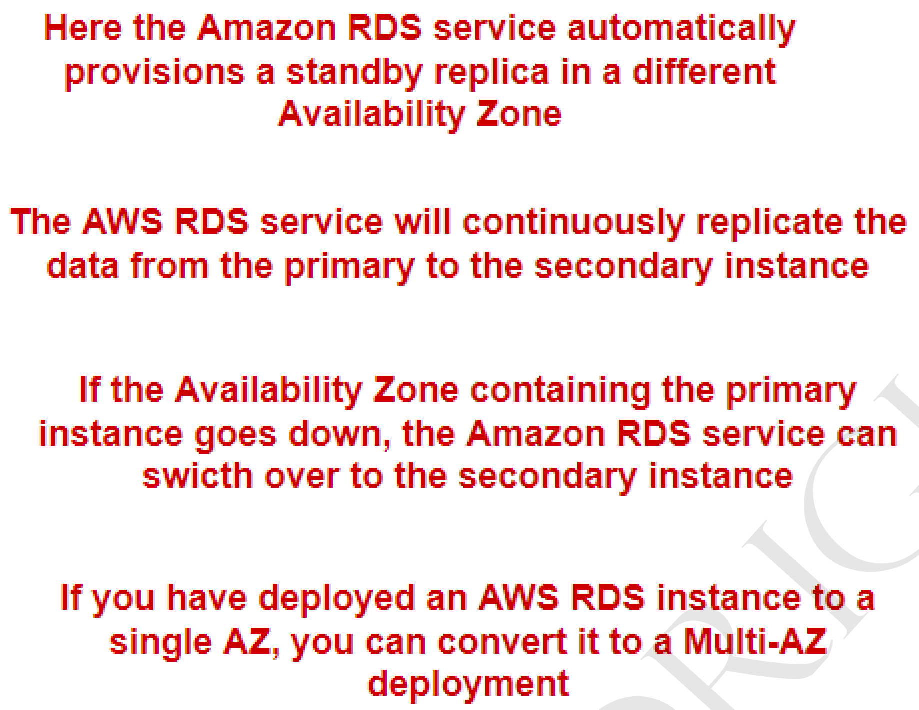


Amazon Relational Database service



Primary Instance

Secondary Instance



Here the Amazon RDS service automatically provisions a standby replica in a different Availability Zone

The AWS RDS service will continuously replicate the data from the primary to the secondary instance

If the Availability Zone containing the primary instance goes down, the Amazon RDS service can swicth over to the secondary instance

If you have deployed an AWS RDS instance to a single AZ, you can convert it to a Multi-AZ deployment

AWS Well-Architected Framework

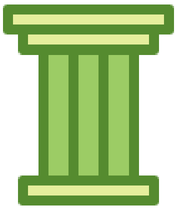
AWS Well-Architected Framework

It always important to architect your applications properly

AWS has guidelines when it comes a framework that can be used when building and hosting applications on the AWS Cloud

These guidelines are based on the time AWS has spent helping their customer adopt the cloud platform.

Pillars of the AWS Well-Architected Framework



Operational Excellence

1. Perform operations as code

2. Make frequent, small , reversible changes

3. Refine operations procedures frequency

4. Anticipate failure

5. Learn from operational failures

Security

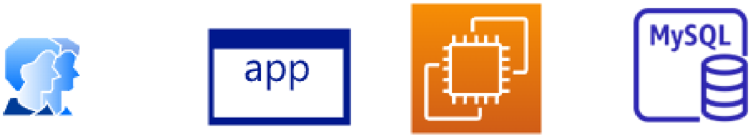
1. Implement a strong identity foundation

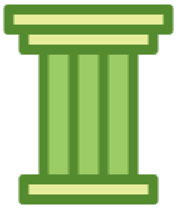
2. Traceability

3. Security at all layers

4. Automate security best practices

5. Protect your data in transit and an in rest





Reliability

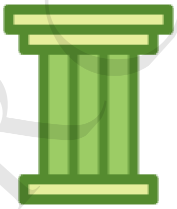
1. Automatically recover from failure

2. Test the Recovery procedures

3. Scale horizontally

4. Stop guessing capacity

5. Manage your infrastructure changes via automation



Performance Efficiency

1. Democratize advanced technologies

2. Go global in minutes

3. Use serverless architecture

4. Perform experimentation

Amazon DynamoDB

AWS Lambda

Cost Optimization

1. Perform Cloud Financial Management

2. Use the Comsumption Model

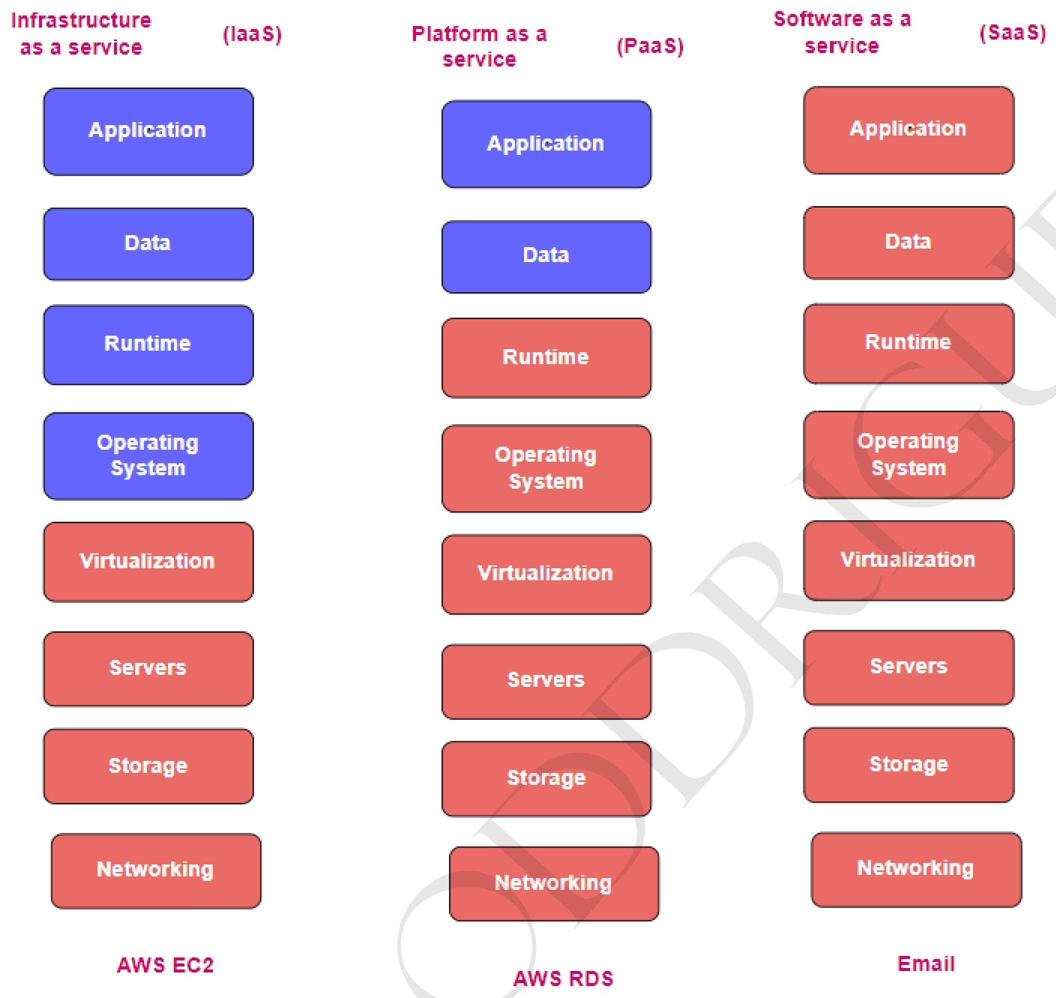
3. Measure overall efficiency

AWS Lambda

Sustainability

1. Establish sustainability goals
2. Understand the impact
3. Maximize utilization

Cloud Computing Model

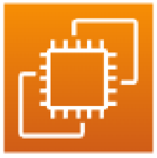


Cloud Computing Deployment Models

Cloud Computing Deployment Models

Cloud **On-premises** **Hybrid**

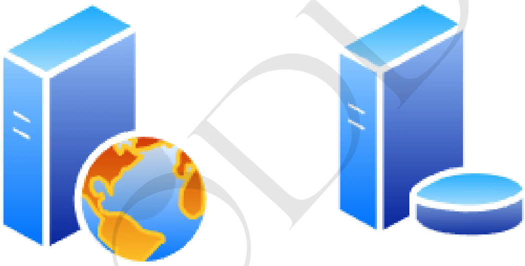
Cloud



EC2 Instance

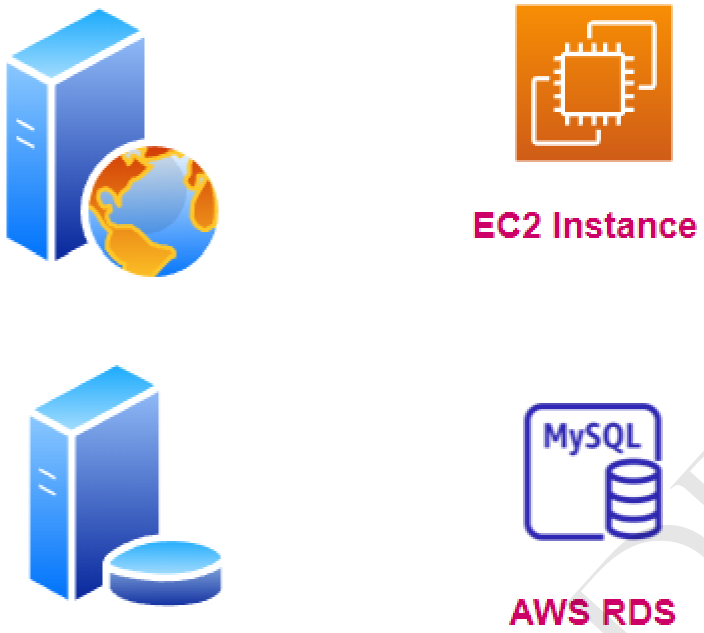
AWS RDS

On-premises



The company has their own data center. They are hosting their own servers

Hybrid Cloud



Domain - Billing and Pricing

Instance pricing

On-demand pricing

EC2 Instance

Pay based on how much you use

There is cost per hour

Spot Instances

This makes use of spare EC2 capacity

If the capacity is available, then you can launch an EC2 Instance

Here the advantage is that the cost of an EC2 Instance is less than the on-demand pricing

And less say that you do get an EC2 Instance based on the available capacity

If AWS needs the capacity back, then the compute capacity is taken back

Hence the workloads running on the Spot Instances should be flexible and be able to run from there left off.

Reserved Pricing

EC2 Instance

Instance type - t2.large

Region - London

Operating System - Linux Distribution

The application is going to run 24*7 throughout the year

Hence you know that this instance type is always required

You can opt for a reserved pricing to be applied to the instance

This helps to significantly save on costs

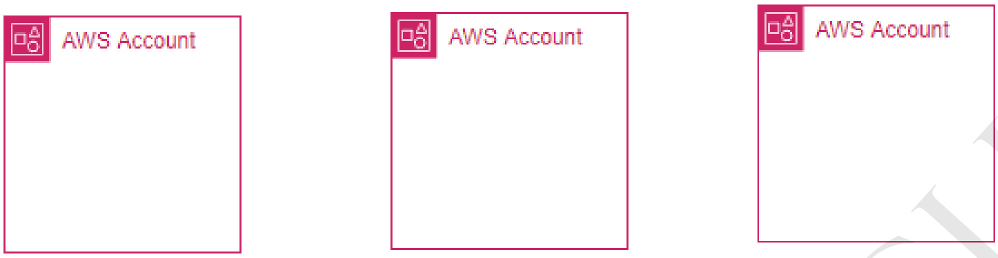
You have to make a one-year or three-year commitment

There are different payment options

There are different class offerings

AWS Consolidated billing

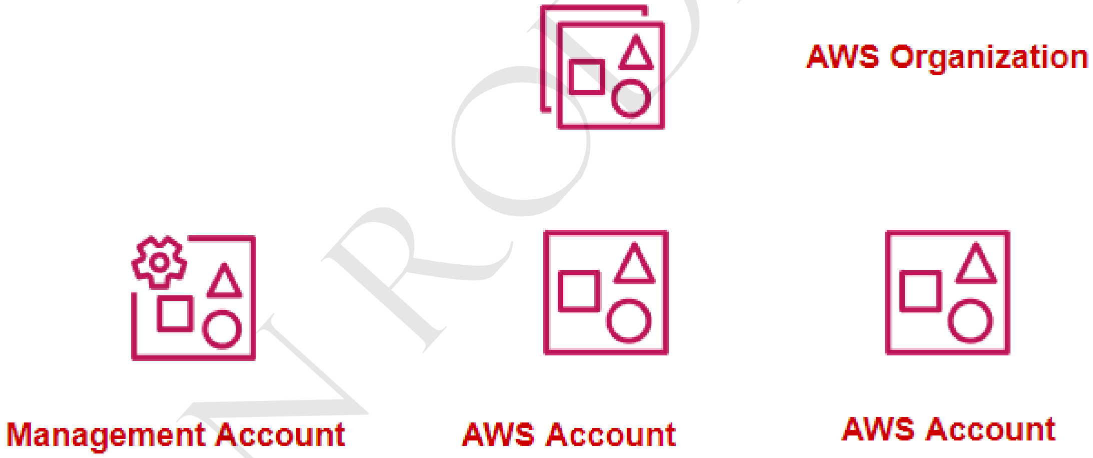
Consolidated billing



A company might have multiple AWS Accounts

There could be an individual account for each key department in a company

You can consolidate the bills from each department and just pay one bill.



You can consolidate the bills from each department